Arithmetik nicht-hyperelliptischer Kurven des Geschlechts 3 und ihre Anwendung in der Kryptographie

Roger Oyono

Dissertation

Arithmetik nicht-hyperelliptischer Kurven des Geschlechts 3 und ihre Anwendung in der Kryptographie

Dissertation zur Erlangung des Grades
eines Doktors der Naturwissenschaften

Dem Fachbereich 6
(Mathematik und Informatik)
der Universität Duisburg-Essen

vorgelegt von

Roger Oyono
aus Yaoundé (Kamerun)

Essen, 2. November 2005

Tag der Disputation: 25.01.2006

Prüfungsvorsitzender: Prof. Dr. Lisa Hefendehl-Hebeker

1. Gutachter: Prof. Dr. Dr. h.c. Gerhard Frey

2. Gutachter: Prof. Dr. Enric Nart

Hiermit erkläre ich, dass ich diese Arbeit selbständig verfasst und keine anderen als die angegebenen Quellen verwendet habe.

Roger Oyono,
Essen, den 2. November 2005

Für meine Eltern

„Sein und Wissen ist ein uferloses Meer: Je weiter wir vordringen, um so unermesslicher dehnt sich aus, was noch vor uns liegt; jeder Triumph des Wissens schließt hundert Bekenntnisse des Nichtwissens in sich.“

Isaac Newton, 1727

Kurzdarstellung der Dissertation

Die vorliegende Dissertation beschäftigt sich mit nicht-hyperelliptischen Kurven vom Geschlecht 3 und möglichen Anwendungen in der Kryptographie.

Der erste Teil der Dissertation hat das Ziel, nicht-hyperelliptische Kurven vom Geschlecht 3 praktikabler für die Kryptographie zu machen. Darunter verstehen wir die Konstruktion eines effizienten Algorithmus zur Berechnung der Gruppenoperation in der Jacobischen generischer nicht-hyperelliptischer Kurven vom Geschlecht 3. Für eine generische nicht-hyperelliptische Kurve mit mindestens einem rationalen Weierstrass-Punkt besitzt der von uns beschriebene Algorithmus eine Komplexität von $148M + 15SQ + 2I$ für eine *Addition* und $165M + 20SQ + 2I$ für eine *Verdopplung*, dabei stehen die Abkürzungen M, SQ, I für Multiplikationen, Quadrierungen und Inversionen.

Im zweiten Teil dieser Dissertation beschäftige ich mich mit der Konstruktion kryptographisch geeigneter Jacobischer nicht-hyperelliptischer Kurven vom Geschlecht 3. Anstatt den naiven und im allgemeinen schwierigen Ansatz der Bestimmung der Anzahl der Punkte einer beliebigen Kurve zur Konstruktion kryptographisch geeigneter Kurven zu verwenden, beschränken wir uns auf eine Alternative, basierend auf $\mathbb{Q}$-einfachen Faktoren A_f der Jacobischen Modulkurven $X_0(N)$: In diesem Fall ist die Anzahl der Punkte von $A_f/\mathfrak{p}$ für Primideale $\mathfrak{p}$ mit guter Reduktion mittels der Theorie von Eichler-Shimura effizient berechenbar. Falls A_f zusätzlich absolut einfach und prinzipal polarisiert ist, existiert eine (bis auf Isomorphie eindeutig bestimmte) Kurve C_f mit $\mathrm{Jac}(C_f) \simeq_{\mathbb{C}} A_f$. Durch das Verschwindungsverhalten gerader Thetanullwerte kann man für $g = 3$ leicht entscheiden, ob die entsprechende Kurve hyperelliptisch ist oder nicht. In dieser Arbeit beschreiben wir zwei verschiedene Methode, die Gleichung der gesuchten Kurve zu berechnen: die eine basiert auf der Berechnung der kanonischen Einbettung mittels einer Basis des Raumes der Spitzenformen $S_2(A_f)$, die andere auf der Berechnung des Riemann-Modells via Auswertungen von Thetafunktionen an ungeraden 2-Torsionspunkten von A_f als komplexer Torus mit Periodenmatrix Ω_f.

Danksagung

Mein besonderer Dank gebührt meinem Doktorvater, Herrn Prof. Dr. Dr. h.c. Gerhard Frey, der die vorliegende Arbeit nicht nur grundsätzlich ermöglicht und die interessante Thematik vorgeschlagen, sondern die Entwicklung der Arbeit mit hilfreichen Gesprächen und fruchtbaren Anregungen stets konstruktiv begleitet hat. Allen Doktoranden und Mitarbeitern des Institutes für Experimentelle Mathematik, insbesondere Guido Blady, Dr. Claus Diem, Dr. Ralph Gerkmann, Oscar Ledesma, Jon Wong Lee, Sebastian Leske, Maxim Li, Dr. Wolfgang Happle, Dr. Sami Omar, Xavier Taixés und Frau Julia Thiemann, danke ich für das freundliche und angenehme Umfeld, welches ein hervorragendes Arbeitsklima geschaffen hat. Außerdem möchte ich mich bei Dr. Stéphane Flon und Dr. Christophe Ritzenthaler für die konstruktive Zusammenarbeit bei der Erarbeitung unserer gemeinsamen Veröffentlichungen bedanken.

Herrn Prof. Dr. Enric Nart möchte ich für die Bereitschaft danken, diese Arbeit als Zweitgutachter anzunehmen.

Bei der Arbeitsgruppe Zahlentheorie der Universität Autònoma de Barcelona bedanke ich mich für die Gastfreundschaft während meines sechsmonatigen Forschungsaufenthaltes von Oktober 2004 bis März 2005. Die dort entstandenen Kontakte sowie das Interesse an meiner Arbeit gaben mir weitere Anstöße für meine Forschung.

Für inspirierende Gespräche danke ich Dr. Roberto Avanzi, Prof. Dr. Gebhard Böckle, Dr. Jordi Guàrdia, Prof. Dr. Josep González, Dr. Tanja Lange, Dr. Annegret Weng und Prof. Dr. Xavier Xarles.

Ganz besonderer Dank geht an Alp Bassa und Björn Buth für das mühsame und sorgfältige Lesen des Manuskriptes.

Ohne die finanzielle Unterstützung durch die Deutsche Forschungsgemeinschaft (DFG), das Graduiertenkolleg „Mathematische und ingenieurwissenschaftliche Methoden für sichere Datenübertragung und Informationsvermittlung“ und die „Marie Curie Research Training Networks“ wäre diese Promotion nicht möglich gewesen.

Schließlich möchte ich mich bei allen Familienmitgliedern und Freunden für die entgegengebrachte Ermunterung und Unterstützung bedanken, ohne die diese Arbeit niemals zustandegekommen wäre.

Und nicht zuletzt danke ich Laure.

Inhaltsverzeichnis

Kapitel 1

Einführung

Motivation

Schon immer bestand die Notwendigkeit, Verfahren zu entwickeln, um geheime Nachrichten vor neugierigen Blicken zu schützen. Früher wurde die Kryptographie den Geheimdiensten und dunklen Kreisen zugeordnet, heute ist sie ein nicht mehr wegzudenkender Bestandteil für offene Netzwerke wie das Internet. Als Folge des zunehmenden Datenverkehrs auf öffentlichen, ungesicherten Netzen werden die Benutzer hinsichtlich der Abhör- und Manipulationssicherheit persönlicher Daten zunehmend sensibler. Insbesondere Anwendungen im Bereich des E-Commerce werden sich nur dann durchsetzen, wenn vertrauliche Informationen sicher über öffentliche Medien ausgetauscht werden können. Die Basistechnologie hierzu ist die Public-Key-Kryptographie. Die Sicherheit von Public-Key-Verfahren beruht auf der Schwierigkeit, bestimmte mathematische Probleme effizient zu lösen.
Die meisten verwendeten Kryptosysteme und Protokolle, wie z.B. das Diffie-Hellman-Protokoll, basieren entweder auf dem Faktorisierungsproblem oder auf dem diskreten Logarithmusproblem (DLP) in endlichen Gruppen: Sei G eine Gruppe und $g \in G$ ein Element dieser Gruppe,

$$\text{zu} \quad g' \in \langle g \rangle \quad \text{bestimme ein} \quad n \in \mathbb{N} \quad \text{mit} \quad g' = g^n.$$

Die bis dato bekannten generischen Algorithmen zur Lösung des DLP in endlichen Gruppen (wie z.B. Baby-Step-Giant-Step, Pollard ρ und Kangaroo, Pohlig-Hellman) haben eine Laufzeit von $O(\sqrt{l})$, wobei l der größte Primfaktor der Gruppenordnung ist. Damit eine Gruppe G kryptographisch geeignet ist, müssen folgende notwendige Bedingungen erfüllt sein:

- die Gruppen-Elemente $g \in G$ sind einfach und kompakt darstellbar,

- die Arithmetik in G ist effizient,
- das DLP in der Gruppe G ist nicht *beherrschbar*,
- die Gruppenordnung $\#G$ ist effizient berechenbar.

Elliptische Kurven über endlichen Körpern $\mathbb{F}_q$ liefern ein großes Arsenal an kryptographisch geeigneten Gruppen, und wurden deshalb im Jahre 1987 durch Koblitz [52] und Miller [62] unabhängig voneinander in der Kryptographie eingeführt. Für sorgfältig gewählte elliptische Kurven sind bis dato keine Algorithmen zur Lösung des DLP bekannt, deren Laufzeit die der generischen Algorithmen schlägt. Inzwischen hat sich das DLP auf elliptischen Kurven etabliert, und ist mittlerweile auch schon reif für die Verwendung in der Industrie: Institutionen wie ANSI, ISO oder IEEE haben bereits fertige Standards für ECC (*elliptic curve cryptography*) erarbeitet.
Eine natürliche Alternative zur ECC ist die Untersuchung des DLP auf Abelschen Varietäten über endlichen Körpern. Die Menge der $\mathbb{F}_q$-rationalen Punkte einer Abelschen Varietät über $\mathbb{F}_q$ bildet eine endliche Abelsche Gruppe und die Addition ist stets durch rationale Funktionen gegeben. Demnach können auch Abelsche Varietät für die DLP-Kryptosysteme genutzt werden. Dabei nennen wir eine über einem endlichen Körper $\mathbb{F}_q$ definierte Abelsche Varietät A geeignet, falls die Gruppe $A(\mathbb{F}_q)$ der $\mathbb{F}_q$-rationalen Punkte kryptographisch geeignet ist. Für ihre kryptographische Anwendung müssen noch die folgende Probleme gelöst werden:

(1) Herleitung einer schnellen Addition auf einer Abelschen Varietät,
(2) Generierung kryptographisch sicherer Abelscher Varietäten.

Die Addition auf einer beliebigen Abelschen Varietät ist im allgemeinen viel zu kompliziert. In einer besseren Situation ist man, wenn die Abelsche Varietät A die Jacobische Varietät $\mathrm{Jac}(C)$ einer Kurve C über $\mathbb{F}_q$ ist. Dann ist die Gruppe $\mathrm{Jac}(C)(\mathbb{F}_q)$ der $\mathbb{F}_q$-rationalen Punkte der Jacobischen Varietät gleich der Divisorenklassengruppe der Kurve C. Durch den Satz von Riemann-Roch lässt sich die Arithmetik auf $\mathrm{Jac}(C)(\mathbb{F}_q)$ auf das Auffinden von Funktionen auf der Kurve mit gegebenen Null- und Polstellen zurückführen. Der Algorithmus von Cantor [10] liefert z.B. eine effiziente Methode zur Addition in der Jacobischen hyperelliptischer Kurven.
Der entscheidende Vorteil der Nutzung Jacobischer Varietäten besteht darin, dass man bei gleichen Sicherheitsanforderungen des Kryptosystems mit deutlich kürzeren Schlüssellängen als bei herkömmlichen Public-Key-Kryptosystem

wie zum Beispiel RSA auskommt. Jacobische Varietäten werden dann besonders interessant, wenn die Speicher- oder Rechenkapazität begrenzt ist, wie z.B. bei Smartcards. Allerdings existieren für Kurven höheren Geschlechts ($g \geq 4$) subexponentielle Algorithmen zum Brechen des DLP (siehe [1, 9, 28, 23, 93]).
Für elliptische bzw. hyperelliptische Kurven vom Geschlecht $g \leq 3$ kann der Algorithmus von Cantor zur Addition in $\mathrm{Jac}(C)(\mathbb{F}_q)$ durch explizite Formeln ersetzt werden [58, 61, 54, 30, 72, 39].
Das Problem der Realisierung einer geeigneten Jacobischen Varietät reduziert sich auf die Realisierung der zugehörigen Kurve. Auch Methoden zur Realisierung geeigneter hyperelliptischer Kurven vom Geschlecht $g \leq 3$ existieren [89, 97, 99].

Im Gegensatz zum Geschlecht 1 bzw. 2, sind nicht alle Kurven vom Geschlecht 3 hyperelliptisch. Im Gegenteil, sind sogar die meisten Kurven vom Geschlecht 3 nicht-hyperelliptisch.

In dieser Arbeit beschäftigen wir uns ausschließlich mit den nicht-hyperelliptischen Kurven vom Geschlecht 3, und werden die beiden oben genannten Probleme (1) und (2) genauer untersuchen.

Inhalt der Arbeit

Der erste Teil der Dissertation hat das Ziel nicht-hyperelliptische Kurven vom Geschlecht 3 praktikabler für die Kryptographie zu machen. Darunter verstehen wir die Konstruktion eines effizienten Algorithmus zur Berechnung der Gruppenoperation in der Jacobischen generischer nicht-hyperelliptischer Kurven vom Geschlecht 3.
Volcheck [95], Huang und Ierardi [45] haben Algorithmen für die Addition auf der Jacobischen beliebiger Kurven vorgeschlagen. Allerdings sind die erwähnten Methoden nicht effizient genug und benötigen ferner eine Arithmetik in Erweiterungskörpern.
Ebenso haben die auf allgemeine Kurven anwendbaren Methoden von Makdisi [51] und Heß [41] eine zu große Laufzeit für eine effiziente Implementierung in der Kryptographie.
Für spezielle Kurven, insbesondere Picard-Kurven, existieren zwar effizientere Methoden, die aber hinsichtlich der Effizienz nicht mit HECC (*hyperelliptic curve cryptography*) konkurieren können [74].
In Zusammenarbeit mit S. Flon und C. Ritzenthaler [24, 25] entwickelte ich einen effizienten Algorithmus zur Addition auf der Jacobischen generischer nicht-

hyperelliptischer Kurven vom Geschlecht 3. Die Komplexität dieses Algorithmus wird durch explizite Formeln erheblich reduziert, so dass sie im Vergleich zu den bis dato publizierten Formeln am effizientesten ist. Dies wird im ersten Teil der Arbeit ausführlich dargestellt.

Im zweiten Teil dieser Dissertation beschäftige ich mich mit der Konstruktion kryptographisch geeigneter Jacobischer nicht-hyperelliptischer Kurven vom Geschlecht 3.
Ein notwendiges Kriterium für die Sicherheit eines Kryptosystems basierend auf dem DLP ist, dass die Gruppenordnung der zugrundeliegenden Gruppe einen *großen* Primfaktor enthält. Aus diesem Grund ist die Bestimmung der Gruppenordnung eine wichtige Aufgabe. Allerdings ist sie im Fall von Jacobischen von Kurven oft ein nicht-triviales Problem: Im Gegensatz zu Kurven über Körpern kleiner Charakteristik [50, 17, 79] ist kein Algorithmus bekannt, der die Ordnung einer zufällig gewählten, kryptographisch geeigneten Jacobischen (der Dimension $g \geq 2$) über einem Primkörper großer Charakteristik ermittelt.

Als Alternative zur Konstruktion kryptographisch geeigneter Jacobischer über großen Primkörpern, wurde von A. Weng [99] der vielversprechende Ansatz der Verwendung hyperelliptischer Kurven vom Geschlecht $g \leq 3$ mit komplexen Multiplikation vorgeschlagen. Die dort erzielten Ergebnisse wurden auch auf Picard-Kurven übertragen [53].
Ich werde in dieser Dissertation den in [96, 97, 34] vorgeschlagenen Weg eingehen. Dazu betrachte ich die $\mathbb{Q}$-einfachen Faktoren A_f des neuen Teils $J_0^{\text{neu}}(N)$ der Jacobischen der Modulkurve $X_0(N)$. In diesem Fall ist die Anzahl der Punkte von $A_f/\mathfrak{p}$ für Primideale $\mathfrak{p}$ mit guter Reduktion mittels der Theorie von Eichler-Shimura effizient berechenbar. Ist A_f zusätzlich absolut einfach und (bezüglich der auf $J_0(N)$ induzierten Polarisierung) prinzipal polarisiert, so existiert eine (bis auf Isomorphie eindeutig bestimmte) Kurve C_f mit $\mathrm{Jac}(C_f) \simeq_{\mathbb{C}} A_f$ [98]. Durch das Verschwindungsverhalten gerader Thetanullwerte kann man für $g = 3$ leicht entscheiden, ob die entsprechende Kurve hyperelliptisch ist oder nicht. Meine Hauptaufgabe bestand darin, die Gleichung einer solchen Kurve zu ermitteln.
Zur Lösung dieses Problems werde ich zwischen *modularen Kurven* und *modularen Jacobischen* unterscheiden, und werde entsprechend zwei verschiedene Wege eingehen: der eine basiert auf der Berechnung der kanonischen Einbettung mittels einer Basis des Raumes der Spitzenformen $S_2(A_f)$, der andere auf der Berechnung des Riemann-Modells via Auswertungen von Thetafunktionen an ungeraden 2-Torsionspunkten von A_f als komplexen Torus mit Periodenmatrix Ω_f.

Die Arbeit ist wie folgt aufgebaut:

Kapitel 2 beschäftigt sich ausführlich mit den Grundlagen über Abelschen Varietäten. Insbesondere werden wir Jacobische Varietäten und ihre Darstellung als Divisorenklassengruppe von Kurven einführen sowie den Zusammenhang zwischen dem Satz von Riemann-Roch und der Realisierung der Gruppenoperation erläutern.

Kapitel 3 beschäftigt sich mit der Arithmetik nicht-hyperelliptischer Kurven vom Geschlecht 3. Nachdem zuerst einige wichtige arithmetische Eigenschaften nicht-hyperelliptischer Kurven eingeführt wurden, werden wir uns hauptsächlich mit der Konstruktion eines effizienten Algorithmus für die Gruppenoperation auf Jacobischen nicht-hyperelliptischer Kurven vom Geschlecht 3 befassen.

In Kapitel 4 beschreiben wir eine konstruktive Methode für den Satz von Torelli in Dimension 3.

Als Anwendung von Kapitel 4 betrachten wir in Kapitel 5 nur die Abelschen Varietäten A_f, die als $\mathbb{Q}$-einfache Faktoren der Jacobischen Modulkurven $X_0(N)$ auftreten. Für *modulare Kurven* werden wir eine andere Methode beschreiben, die mittels einer Basis aus Spitzenform von $S_2(A_f)$ die Gleichung einer Kurve C_f mit $\mathrm{Jac}(C_f) \sim_{\mathbb{Q}} A_f$ berechnet.

Kapitel 2

Algebraische Kurven und Jacobische Varietäten

2.1 Abelsche Varietäten

In diesem Abschnitt verstehen wir unter einer Varietät über einem Körper k stets eine absolut irreduzible Varietät.

2.1.1 Gruppengesetz

Definition 2.1.1. Eine (absolut irreduzible) **algebraische Gruppe** $\mathcal{G}$ über einem Körper k ist eine absolut irreduzible Varietät über k zusammen mit

(i) einem über k definierten Morphismus (Addition) $\quad m : \mathcal{G} \times \mathcal{G} \longrightarrow \mathcal{G}$,

(ii) einem über k definierten Morphismus (Inversion) $\quad i : \mathcal{G} \longrightarrow \mathcal{G}$,

(iii) einem k-rationalen Punkt (neutrales Element) $\quad 0 \in \mathcal{G}(k)$,

so dass die gewöhnlichen Gruppengesetze

$$m \circ (\mathrm{id}_{\mathcal{G}} \times m) = m \circ (m \times \mathrm{id}_{\mathcal{G}}) \quad \text{(Assoziativität)},$$

$$m_{|\{0\}\times\mathcal{G}} = \mathrm{pr}_2,$$

und

$$m \circ (i \times \mathrm{id}_{\mathcal{G}}) \circ \delta_{\mathcal{G}} = c_0,$$

erfüllt sind. Dabei sind pr_2 die Projektion von $\mathcal{G} \times \mathcal{G}$ auf den zweiten Faktor, $\delta_{\mathcal{G}}$ die *Diagonalabbildung* von $\mathcal{G}$ nach $\mathcal{G} \times \mathcal{G}$, und c_0 die *Nullabbildung*.

Sei E ein Erweiterungskörper von k und $\mathcal{G}(E)$ die Menge der E-rationalen Punkte von $\mathcal{G}$. Die Menge $\mathcal{G}(E)$ bildet eine Gruppe, indem Addition und Inverse durch Auswertungen von k-Morphismen berechnet werden.

Im folgenden verwenden wir die Bezeichnungen $P \oplus Q := m(P, Q)$ und $-P := i(P)$ für alle $P, Q \in \mathcal{G}(\bar{k})$.

Ist die algebraische Gruppe $\mathcal{G}$ projektiv, so ist sie notwendigerweise kommutativ (siehe [55, p. 20]).

Definition 2.1.2. Eine **Abelsche Varietät** ist eine projektive algebraische Gruppe.

Sei A eine Abelsche Varietät über k. Dann gibt es affine Untervarietäten V_i, die A überdecken. Sei $V := V_i$ eine solche Untervarietät, und seien $X_1, \ldots, X_l$ Koordinatenfunktionen, so dass V durch Polynome

$$f_1(X_1, \ldots, X_l), \ldots, f_n(X_1, \ldots, X_l)$$

definiert ist. Sei E eine Erweiterung von k. Die Menge der E-rationalen Punkte $V(E) \subset A(E)$ besteht aus den Elementen $x := (x_1, \ldots, x_l) \in E^l$ mit $f_i(x) = 0$ für alle $i \in \{1, \ldots, n\}$. Das Gruppengesetz kann auf $V \times V$ eingeschränkt werden und induziert den Morphismus

$$m_V : \ V \times V \longrightarrow A.$$

Das Bild von generischen Punkten aus $V \times V$ unter m_V ist wieder in V enthalten. Der Morphismus m_V ist dann durch rationale Funktionen $R_i \in k(X_1, \ldots, X_l; Y_1, \ldots, Y_l)$ gegeben, welche den Punkt $(x; y) = (x_1, \ldots, x_l; y_1, \ldots, y_l) \in V \times V$ auf den Punkt

$$x \oplus y = (R_1(x; y), \ldots, R_l(x; y))$$

abbildet.

Bemerkung 2.1.1. Diese birationale Beschreibung des Gruppengesetzes gilt außerhalb einer abgeschlossenen Untervarietät von $V \times V$ echt positiver Kodimension. Insbesondere ist die Wahrscheinlichkeit groß, dass an ein zufälliges Punktepaar $(P, Q) \in (V \times V)(\bar{k})$ das birationale Gruppengesetz anwendbar ist.

Mit dem Ziel Abelsche Varietäten als Gruppen für Kryptosysteme basierend auf dem DLP zu verwenden, brauchen wir nicht nur ihre abstrakte Struktur als Gruppe, sondern auch eine explizite Darstellung ihrer Elemente sowie eine explizite

und effiziente Realisierung des Gruppengesetzes. Dies scheint i.A. aussichtslos zu sein: Mumford [67] und Lange-Ruppert [57] haben bewiesen, dass die Anzahl der Koordinatenfunktionen und der Grad der Additionsformeln exponentiell in Abhängigkeit der Dimension der Abelschen Varietäten wachsen. Für kryptographische Anwendungen brauchen wir aber Abelsche Varietäten, in denen wir das Additionsgesetz (zumindest in einem affinen Teil) leicht und effizient beschreiben können.

Man ist in einer besseren Situation, wenn die Abelsche Varietät A die Jacobische Varietät $\mathrm{Jac}(C)$ einer glatten projektiven Kurve C ist.

2.1.2 Isogenien

Für weitere Details sowie vollständige Beweise verweisen wir in diesem Abschnitt auf das Buch von Lang [55].

Seien A und B zwei Abelsche Varietäten über $\bar{k}$. Der Kern eines Homomorphismus $I : A \longrightarrow B$ ist definiert durch

$$\mathrm{Kern}(I) := \{a \in A : \ I(a) = e_B \in B\},$$

wobei e_B das neutrale Element von B ist.

Proposition 2.1.1. Ein Homomorphismus $I : A \longrightarrow B$ von Abelschen Varietäten A und B heißt **Isogenie**, falls er surjektiv ist und einen endlichen Kern $\mathrm{Kern}(I)$ hat. Für einen Homomorphismus $I : A \longrightarrow B$ sind die folgenden Aussagen äquivalent:

(i) I ist eine Isogenie,
(ii) $\dim(A) = \dim(B)$ und I ist surjektiv,
(iii) $\dim(A) = \dim(B)$ und $\mathrm{Kern}(I)$ ist endlich.

Der **Grad** einer Isogenie I ist definiert als sein Grad als Morphismus zwischen algebraischen Varietäten. Ist der Grad von I teilerfremd zu $\mathrm{char}(k)$, so gilt

$$\mathrm{Grad}(I) = \#\mathrm{Kern}(I)(\bar{k}).$$

Beispiel 2.1.1. Sei A eine Abelsche Varietät über $\mathbb{F}_{p^n}$ der Dimension g und $m \in \mathbb{N}$ teilerfremd zu p. Die Multiplikation mit m, definiert durch

$$[m]_A(P) := \underbrace{P + \cdots + P}_{m-\mathrm{mal}},$$

ist eine Isogenie von A. Der Kern von A hat Ordnung m^{2g}.

Die Menge $\mathrm{Hom}(A, B)$ der Isogenien von A nach B bildet eine Gruppe mit dem Additionsgesetz

$$(I_1 + I_2)(a) = I_1(a) + I_2(a).$$

Die Untergruppe der Isogenien in $\mathrm{Hom}(A, B)$, die über k definiert sind, bezeichnen wir mit $\mathrm{Hom}_k(A, B)$. Die Gruppe $\mathrm{End}(A)$ der Endomorphismen von A bildet einen Ring mit der Multiplikation

$$(I_1 \cdot I_2)(a) = I_1\left(I_2(a)\right).$$

Satz 2.1.1. Sei $I : A \longrightarrow B$ eine Isogenie vom Grad d zwischen zwei Abelschen Varietäten A und B. Dann gibt es eine Isogenie $\hat{I} : B \longrightarrow A$, so dass

$$\hat{I} \circ I = [d]_A \quad \text{und} \quad I \circ \hat{I} = [d]_B.$$

Wir nennen zwei Abelsche Varietäten A und B **isogen**, im Zeichen $A \sim B$, wenn zwischen ihnen eine Isogenie $I : A \longrightarrow B$ existiert.

Definition 2.1.3. Eine Abelsche Varietät A heißt **einfach**, falls sie keine echte Abelsche Untervarietät enthält, d.h. wenn $\{0\}$ und A ihre einzigen Abelschen Untervarietäten sind.

Abelsche Varietäten kann man zerlegen, diese Zerlegung ist bis auf Isogenie eindeutig:

Satz 2.1.2. Jede Abelsche Varietät A ist isogen zu einem Produkt von Abelschen Varietäten

$$A \sim A_1^{n_1} \times \cdots \times A_m^{n_m},$$

wobei die A_i paarweise nicht-isogene einfache Abelsche Varietäten sind. Diese Zerlegung ist bis auf Isogenie eindeutig bestimmt.

Alle bis jetzt erwähnten Ergebnisse sind nur über algebraisch abgeschlossenen Körper zutreffend. Zwei Abelsche Varietäten heißen k-isogen, falls zwischen ihnen eine Isogenie über k existiert. In diesem Fall bleibt der Zerlegungssatz richtig. Es kann aber Abelsche Varietäten geben, die über k einfach sind, jedoch über $\bar{k}$ nicht mehr einfach sind.

Definition 2.1.4. Eine Abelsche Varietät A heißt **absolut einfach**, falls sie über $\bar{k}$ einfach ist.

Proposition 2.1.2. Falls A einfach ist, so ist $\mathrm{End}_k(A)$ ein nullteilerfreier Ring und $\mathrm{End}_k^0(A) := \mathrm{End}_k(A) \otimes \mathbb{Q}$ ein Schiefkörper.

Ist $k = \mathbb{F}_{p^n}$ und A eine über k definierte Abelsche Varietät der Dimension g, so heißt A **supersingulär** genau dann, wenn es eine supersinguläre elliptische Kurve E (d.h. eine elliptische Kurve E mit $\mathrm{rang}_p(E) = 0$) gibt, so dass $A \sim_{\bar{k}} E^g$.

2.2 Jacobische Varietäten

2.2.1 Divisoren

Im folgenden sei k ein perfekter Körper und $\bar{k}$ ein algebraischer Abschluss von k. Sei C eine vollständige glatte absolut irreduzible Kurve über k. Wir schreiben kurz $P \in C$ für $P \in C(\bar{k})$.

Die **Divisorengruppe** $\mathrm{Div}(C)$ von C ist die (additiv geschriebene) freie Abelsche Gruppe, die durch die Punkte von C erzeugt wird. Ihre Elemente heißen **Divisoren**. Konkret ist ein Divisor eine formale Summe

$$\sum_{P \in C} n_P P$$

mit $n_P \in \mathbb{Z}$ und fast allen $n_P = 0$. Divisoren mit $n_P \geq 0$ für alle $P \in C$ heißen **effektiv (positiv)**. Für $D_1, D_2 \in \mathrm{Div}(C)$ schreiben wir $D_1 \geq D_2$ genau dann, wenn $D_1 - D_2$ positiv ist. Der **Grad** eines Divisors ist die ganze Zahl $\deg(D) = \sum_{P \in C} n_P$. Die Divisoren von Grad 0 bilden eine Untergruppe $\mathrm{Div}^0(C)$ von $\mathrm{Div}(C)$.

Da die Kurve C über k definiert ist, operiert die Galoisgruppe $\mathrm{Gal}(\bar{k}/k)$ auf $\mathrm{Div}(C)$ (und $\mathrm{Div}^0(C)$) trivialerweise durch

$$D^\sigma := \sum_{P \in C} n_P P^\sigma$$

für alle $\sigma \in \mathrm{Gal}(\bar{k}/k)$. Ein Divisor ist über k definiert, falls er invariant unter dieser Galois-Operation ist. Sei $\mathrm{Div}_k(C)$ (bzw. $\mathrm{Div}_k^0(C)$) die aus den über k definierten Divisoren von $\mathrm{Div}(C)$ bestehende Untergruppe.
Ein effektiver Divisor D über k heißt **prim**, falls er außer 0 keinen echten k-Teildivisor enthält.

Zu einer meromorphen Funktion $f \in \bar{k}(C)^*$ assoziieren wir den **Hauptdivisor** (f) definiert durch

$$(f) := \sum_{P \in C} \mathrm{ord}_P(f) P,$$

und für alle $\sigma \in \mathrm{Gal}(\bar{k}/k)$ gilt

$$(f^\sigma) = (f)^\sigma.$$

Insbesondere liegt (f) in $\mathrm{Div}_k(C)$, falls $f \in k(C)^*$ ist.
Die Menge $\mathrm{Princ}(C)$ der Hauptdivisoren bildet eine Untergruppe von $\mathrm{Div}^0(C)$. Zwei Divisoren D_1 und D_2 heißen äquivalent, i.Z. $D_1 \sim D_2$, falls $D_1 - D_2 = (f)$ für ein $f \in \bar{k}(C)^*$ ist.

Die **Divisorenklassengruppe (Picardgruppe)** $\mathrm{Pic}(C)$ ist die Faktorgruppe der Divisorengruppe $\mathrm{Div}(C)$ modulo $\mathrm{Princ}(C)$.

2.2.2 Differentialformen

Definition 2.2.1. Sei C eine vollständige glatte absolut irreduzible Kurve. Der Raum Ω_C der (meromorphen) Differentialformen auf C ist der $\bar{k}(C)$-Vektorraum, der von Symbolen der Form df mit $f \in \bar{k}(C)$ erzeugt wird, modulo der Relationen

(i) $d(x+y) = dx + dy$ für alle $x, y \in \bar{k}(C)$,
(ii) $d(xy) = xdy + ydx$ für alle $x, y \in \bar{k}(C)$,
(iii) $da = 0$ für alle $a \in \bar{k}$.

Der Raum Ω_C ist ein 1-dimensionaler $\bar{k}(C)$-Vektorraum für den gilt:

Proposition 2.2.1. Sei $P \in C$, $t_P \in \bar{k}(C)$ eine Ortsuniformisierende bei P. Dann gilt:

(i) Für alle $\omega \in \Omega_C$ existiert ein $g_{\omega,t_P} \in \bar{k}(C)$ mit $\omega = g_{\omega,t_P} dt_P$.
(ii) Ist $f \in \bar{k}(C)$ regulär bei P so auch df/dt_P.
(iii) $\mathrm{ord}_P(\omega/dt_P)$ hängt nur von P und ω ab. Sei

$$\mathrm{ord}_P(\omega) := \mathrm{ord}_P(\omega/dt_P),$$

dann ist $\mathrm{ord}_P(\omega) = 0$ für fast alle $P \in C$.

Definition 2.2.2. Zum Differential $\omega \in \Omega_C$ wird der Divisor (ω) durch

$$(\omega) := \sum_{P \in C} \mathrm{ord}_P(\omega) P$$

definiert. Das Differential ω heißt **regulär (holomorph)** genau dann, wenn $\mathrm{ord}_P(\omega) \geq 0$ für alle $P \in C$. Mit Ω^1_C bezeichnen wir den Raum

$$\Omega^1_C := \{\omega \in \Omega_C : \omega \text{ holomorph}\}$$

der holomorphen Differentialformen von C.

Für $\omega_1, \omega_2 \in \Omega_C^* = \Omega_C \setminus \{0\}$ existiert ein $f \in \bar{k}(C)^*$ mit $\omega_1 = f\omega_2$, also $(\omega_1) = (f) + (\omega_2) \sim (\omega_2)$. Die folgende Definition ist also sinnvoll:

Definition 2.2.3. Die kanonische Divisorenklasse von C ist das Bild in $\mathrm{Pic}(C)$ von (ω) für alle $\omega \in \Omega_C^*$. Jeder Divisor in dieser Klasse heißt **kanonischer Divisor**.

2.2.3 Der Satz von Riemann-Roch

Zu $D \in \mathrm{Div}(C)$ definiert man den $\bar{k}$-Vektorraum

$$\mathcal{L}(D) := \left\{ f \in \bar{k}(C)^* : \ (f) \geq -D \right\} \cup \{0\}.$$

Der Raum $\mathcal{L}(D)$ ist ein endlich-dimensionaler $\bar{k}$-Vektorraum. Sei $l(D) := \dim_{\bar{k}}(\mathcal{L}(D))$ seine Dimension. Falls C über k definiert ist und $D \in \mathrm{Div}_k(C)$, dann besitzt $\mathcal{L}(D)$ eine Basis in $k(C)$.

Sei $K_C := (\omega) \in \mathrm{Div}(C)$ ein kanonischer Divisor von C. Für alle $f \in \mathcal{L}(K_C)$ gilt $(f) \geq -(\omega)$, d.h. $(f\omega) \geq 0$, also ist $f\omega$ holomorph. Ist umgekehrt $f\omega$ holomorph, so ist $f \in \mathcal{L}(K_C)$. Da jedes Differential von der Form $f\omega$ für ein $f \in \bar{k}(C)$ ist, folgt

$$\mathcal{L}(K_C) \simeq \{\omega \in \Omega_C : \ \omega \text{ holomorph}\} = \Omega_C^1.$$

Die positive ganze Zahl $g := l(K_C)$, die man als das **Geschlecht** der Kurve C bezeichnet, ist eine wichtige Invariante der Kurve C.

Satz 2.2.1 (**Riemann-Roch**). Sei C eine Kurve und K_C ein kanonischer Divisor von C. Dann gilt

$$l(D) - l(K_C - D) = \deg(D) - g + 1.$$

Für einen kanonischen Divisor K_C gilt

$$\deg(K_C) = 2g - 2.$$

Ist D ein Divisor mit $\deg(D) < 0$, so ist $l(D) = 0$. Im Fall $\deg(D) > 2g-2$, hängt $l(D)$ nur von $\deg(D)$ (und vom Geschlecht g) ab; es gilt $l(D) = \deg(D) + 1 - g$. Im Fall $0 \leq \deg(D) \leq 2g - 2$ gelten die folgenden Abschätzungen:

Satz 2.2.2 (**Clifford**). Für einen Divisor D mit $0 \leq \deg(D) \leq 2g - 2$ gilt

$$\deg(D) + 1 - g \leq l(D) \leq 1 + \frac{\deg(D)}{2}.$$

Ein Punkt $P \in C$ mit $l(gP) \geq 2$ heißt **Weierstrass-Punkt**.

2.2.4 Picardgruppen und Jacobische Varietäten

Definition der Jacobischen Varietät

Sei $\mathrm{Pic}_k(C)$ die Untergruppe von $\mathrm{Pic}(C)$, die invariant unter $\mathrm{Gal}(\bar{k}/k)$ ist. Falls wir in der Definition der Divisorenklassengruppe $\mathrm{Div}(C)$ durch $\mathrm{Div}^0(C)$ ersetzen, so erhalten wir $\mathrm{Pic}^0(C)$ und die Untergruppe $\mathrm{Pic}^0_k(C)$. Im allgemeinen ist $\mathrm{Pic}^0_k(C)$ nicht die Faktorgruppe von $\mathrm{Div}^0_k(C)$ modulo $\mathrm{Princ}_k(C)$, aber mit der Restriktion $C(k) \neq \emptyset$ gilt:

Lemma 2.2.1. Sei C eine Kurve über k mit einem k-rationalen Punkt und $D \in \mathrm{Div}^0_k(C)$. Falls eine Funktion $f \in \bar{k}(C)$ mit $D' := D + (f) \in \mathrm{Div}^0_k(C)$ existiert, so gibt es eine Funktion $g \in k(C)$ mit $(f) = (g)$. Insebsondere gilt

$$\mathrm{Pic}^0_k(C) \simeq \mathrm{Div}^0_k(C)/\mathrm{Princ}_k(C).$$

Die wichtigste und eindrucksvollste Eigenschaft der Picardgruppe $\mathrm{Pic}^0(C)$ ist, dass sie geometrisch durch die Jacobische Varietät $\mathrm{Jac}(C)$ von C darstellbar ist. Genauer:

Satz 2.2.3. Sei C eine Kurve vom Geschlecht $g \geq 1$ über k mit einem k-rationalen Punkt. Es gibt eine über k definierte Abelsche Varietät $\mathrm{Jac}(C)$ der Dimension g und einen über k definierten kanonischen Morphismus

$$\Phi : \ C \longrightarrow \mathrm{Jac}(C)$$

mit der folgenden universellen Eigenschaft:
Sei $h : \ C \longrightarrow A$ ein Morphismus von C in eine Abelsche Varietät A. Dann gibt es genau einen Homomorphismus $\alpha : \ \mathrm{Jac}(C) \longrightarrow A$ und ein Element $a \in A$, so dass $h(x) = \alpha(\Phi(x)) + a$ für alle $x \in C$. Diese bis auf Isomorphie eindeutig bestimmte Abelsche Varietät $\mathrm{Jac}(C)$ heißt **Jacobische Varietät** von C und es gilt

$$\mathrm{Jac}(C)(L) \simeq \mathrm{Pic}^0_L(C)$$

für jeden Körper L/k, für den C einen L-rationalen Punkt enthält.

Für die Verwendung in der Public-Key-Kryptographie ist es von großer Bedeutung die Elemente der Jacobischen $\mathrm{Jac}(C)$ in eindeutiger Art und Weise darzustellen. Dies führt zum Begriff des **reduzierten Divisors**.

Darstellung reduzierter Divisoren

Sei im folgenden g das Geschlecht der Kurve C. Für (nicht notwendig verschiedene) k-rationale Punkte $P_1^\infty, \ldots, P_g^\infty$ auf der Kurve C definieren wir die positiven k-Divisoren

$$D_\infty^{(0)} := 0,\ D_\infty^{(i)} := \sum_{k=1}^{i} P_k^\infty,\ i = 1, \ldots, g.$$

Lemma 2.2.2. Zu $D \in \mathrm{Div}_k^0(C)$ existiert ein effektiver Divisor $E \in \mathrm{Div}_k(C)$ mit $D \sim E - D_\infty^{(g)}$. Wir bezeichnen einen solchen Divisor $E - D_\infty^{(g)}$ im folgenden als **semi-reduzierten** Divisor.

Beweis. Sei $D' := D + D_\infty^{(g)}$. Der Satz von Riemann-Roch liefert die Ungleichung

$$l(D') = l(K_C - D') + \deg(D) + \deg(D_\infty^{(g)}) + 1 - g \geq 1.$$

Es existiert also ein $f \in k(C)$ mit $(f) \geq -D'$. Der Divisor $E := (f) + D'$ erfüllt somit die Voraussetzung des gesuchten Divisors. □

Satz 2.2.4. Zu $D \in \mathrm{Div}_k^0(C)$ existiert ein eindeutiger effektiver Divisor $E \in \mathrm{Div}_k(C)$ mit minimalem Grad $m \in \{0, \ldots, g\}$, so dass $D \sim E - D_\infty^{(m)}$. Diesen Divisor bezeichnen wir als kanonischen Repräsentanten (**reduzierter Divisor**) der Divisorenklasse $[D]$.

Beweis. Falls D ein Hauptdivisor ist, so wählen wir $m = 0$ und $E = 0$. Sei also D kein Hauptdivisor. Dann ist $l(D) = 0$. Nach Definition von $\mathcal{L}(D)$ ist $l(D + D_\infty^{(i)})$ monoton wachsend in i. Vergrößert man i um 1, so wächst $l(D + D_\infty^{(i)})$ höchstens um 1, denn nach dem Satz von Riemann-Roch gilt

$$l\left(D + D_\infty^{(m+1)}\right) - l\left(D + D_\infty^{(m)}\right) = l\left(K_C - D - D_\infty^{(m+1)}\right) + 1 - l\left(K_C - D - D_\infty^{(m)}\right).$$

Sei dann m das kleinste Element in $\{0, \ldots, g\}$ mit

$$l(D + D_\infty^{(m)}) = 1$$

und $f \in k(C)$ (bis auf konstanten Faktor eindeutig), so dass

$$\mathcal{L}(D + D_\infty^{(m)}) = \langle f \rangle_{\bar{k}},$$

wobei $\langle f \rangle_{\bar{k}}$ der durch f erzeugte $\bar{k}$-Vektorraum ist.
Der Divisor $E := (f) + D + D_\infty^{(m)}$ erfüllt die Bedingung des Satzes. □

2.2.5 Der Satz von Hasse-Weil

Sei $C/\mathbb{F}_q$ eine vollständige glatte und absolut irreduzible Kurve vom Geschlecht g. Die **Zeta Funktion** von C ist definiert durch

$$Z_C(t) := \exp\left(\sum_{n\geq 1} N_n \frac{t^n}{n}\right),$$

wobei $N_n = \#C(\mathbb{F}_{q^n})$.
Im folgenden geben wir einige bekannte Eigenschaften der Zeta Funktion an:

Satz 2.2.5 (Weil). Die Zeta Funktion einer Kurve $C/\mathbb{F}_q$ vom Geschlecht g erfüllt die folgenden Bedingungen:

(i) **Rationalität**: $Z_C(t)$ ist eine rationale Funktion, genauer

$$Z_C(t) = \frac{L(t)}{(1-t)(1-qt)},\ L(t) \in \mathbb{Z}[t].$$

(ii) **Funktionalgleichung**: $Z_C(t) = q^{g-1}t^{2g-2}Z_C\left(\frac{1}{qt}\right)$.

(iii) **Riemannsche Vermutung**: Die Inversen der Nullstellen von $Z_C(t)$ haben den Betrag $\sqrt{q}$.

Das Polynom $L(t) = (1-t)(1-qt)Z_C(t)$ bezeichnet man als *L-Polynom* der Kurve C. Es genügt:

(iv) $L(t) \in \mathbb{Z}[t]$ mit $\deg(L(t)) = 2g$,

(v) $\#\mathrm{Jac}(C)(\mathbb{F}_q) = L(1)$,

(vi) Für $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$ gilt

- $a_0 = 1,\ a_{2g} = q^g$,
- $a_{2g-i} = q^{g-i}a_i$ für $0 \leq i \leq g$.

(vii) Falls $L(t) = \prod(1-\alpha_i t)$, so gibt es eine Anordnung der α_i, so dass $\alpha_i\alpha_{g+i} = q$. Ferner gilt $|\alpha_i| = \sqrt{q}$.

Betrachtet man $C/\mathbb{F}_q$ als Kurve über $\mathbb{F}_{q^r}$, und kennt man $\#C(\mathbb{F}_{q^r})$ für $r = 1,\ldots,g$, so kann man das L-Polynom von $C/\mathbb{F}_q$ und somit $\#\mathrm{Jac}(C)(\mathbb{F}_q)$ berechnen, denn

$$ia_i = \sum_{j=1}^{i} \left(\#C(\mathbb{F}_{q^j}) - (q^j+1)\right) a_{i-j}$$

für $i = 1,\ldots,g$.

Korollar 2.2.1. Ist $L(t) = \prod(1 - \alpha_i t)$ das L-Polynom von $C/\mathbb{F}_q$, so gilt für die Zeta Funktion $Z_C^{(r)}(t)$ der Kurve $C/\mathbb{F}_{q^r}$

(i) $Z_C^{(r)}(t) = \dfrac{\prod(1 - \alpha_i^r t)}{(1-t)(1-q^r t)}$,

(ii) $|\#C(\mathbb{F}_{q^r}) - (q^r + 1)| \leq 2g\sqrt{q^r}$,

(iii) $(\sqrt{q^r} - 1)^{2g} \leq \#\mathrm{Jac}(C)(\mathbb{F}_{q^r}) \leq (\sqrt{q^r} + 1)^{2g}$,

(iv) $\#\mathrm{Jac}(C)(\mathbb{F}_{q^r}) = \prod_{i=1}^{2g}(1 - \alpha_i^r)$.

Verbindung mit dem Frobenius

Sei $C/\mathbb{F}_q$ weiterhin eine ebene Kurve vom Geschlecht g. Der Frobenius-Automorphismus von $\mathbb{F}_q$ lässt sich wie folgt zu einem Morphismus der Kurve C erweitern:

$$\pi_q : \ C(\overline{\mathbb{F}_q}) \longrightarrow C(\overline{\mathbb{F}_q}), \ (x, y) \longmapsto (x^q, y^q).$$

Der Frobenius π_q induziert auf der Jacobischen $\mathrm{Jac}(C)(\overline{\mathbb{F}_q})$ einen Endomorphismus, den wir auch als Frobenius bezeichnen. Ein Element der Jacobischen $\mathrm{Jac}(C)(\overline{\mathbb{F}_q})$ ist dann über $\mathbb{F}_q$ definiert, falls es unter der Operation der Galoisgruppe $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q)$ invariant ist, d.h. falls es unter dem Frobenius invariant ist.

Satz 2.2.6. Für das charakteristische Polynom $\chi_{\pi_q}(t)$ des Frobenius Endomorphismus auf $\mathrm{Jac}(C/\mathbb{F}_q)$ gilt

$$\chi_{\pi_q}(t) = t^{2g} L\left(\frac{1}{t}\right) \in \mathbb{Z}[t], \ \deg(\chi_{\pi_q}(t)) = 2g.$$

Ferner gilt

$$\#\mathrm{Jac}(C)(\mathbb{F}_q) = \chi_{\pi_q}(1).$$

Eine über $\mathbb{F}_{p^n}$ definierte Kurve C vom Geschlecht g heißt **supersingulär** genau dann, wenn ihre Jacobische $\mathrm{Jac}(C)$ als Abelsche Varietät supersingulär ist. Supersinguläre Kurven lassen sich am charakteristischen Polynom $\chi_{\pi_{p^n}}(t)$ des Frobenius Endomorphismus erkennen: ist nämlich

$$\chi_{\pi_{p^n}}(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_g t^g + \cdots + q^{g-1} a_1 t + q^g,$$

so ist C genau dann supersingulär, wenn

$$p^{\lceil ni/2 \rceil} | a_i$$

für alle $i \in \{1, \cdots, g\}$.

2.2.6 Beispiel: hyperelliptische Kurven und ihre Jacobischen

Definition 2.2.4. Eine Kurve C/k vom Geschlecht g heißt **hyperelliptisch**, falls es einen Morphismus $\varphi : C \longrightarrow \mathbb{P}^1$ vom Grad 2 gibt.

Der Funktionenkörper $k(C)$ von C ist in diesem Fall eine separable Erweiterung vom Grad 2 eines rationalen Funktionenkörpers $k(x)$. Der nicht-triviale Morphismus τ dieser Erweiterung induziert eine Involution von C, die wir im folgenden als **hyperelliptische Involution** bezeichnen. Die Verzweigungspunkte $P_1, \ldots, P_{2g+2}$ von φ sind genau die Fixpunkte der Involution τ. Falls $\mathrm{char}(k) \neq 2$, so entsprechen die Verzweigungspunkte von φ genau den Weierstrass-Punkten der Kurve.

Lemma 2.2.3. Ist C/k eine hyperelliptische Kurve, so besitzt sie ein nicht-singuläres affines Modell, gegeben durch

$$y^2 + h(x)y = f(x)$$

mit $h(x), f(x) \in k[x]$. Die hyperelliptische Involution ist gegeben durch

$$\tau : (x, y) \longmapsto (x, -y - h(x)).$$

Proposition 2.2.2. Sei k ein Körper der Charakteristik $\mathrm{char}(k) \neq 2$ und C/k eine hyperelliptische Kurve vom Geschlecht g. Dann besitzt C ein nicht-singuläres affines Modell

$$y^2 = f(x),$$

wobei das Polynom $f(x) \in k[x]$ quadratfrei ist. Der Grad von $f(x)$ ist entweder $2g + 1$ (*imaginär quadratisch*) oder $2g + 2$ (*reell quadratisch*).

In [22] gibt A. Enge für $\mathrm{char}(k) = 2$ eine vollständige Beschreibung der möglichen affinen Modelle hyperelliptischer Kurven.

In diesem Abschnitt betrachten wir nur hyperelliptische Kurven $C/\mathbb{F}_q$ über endlichen Körpern $\mathbb{F}_q$ der Charakteristik $\mathrm{char}(\mathbb{F}_q) \neq 2$ mit einem $\mathbb{F}_q$-rationalen Weierstrass-Punkt $P_\infty := P_{2g+2}$. In diesem Fall kann man durch eine Variablentransformation $\deg(f) = 2g + 1$ erreichen. Für den Ring

$$\mathcal{O} = \mathbb{F}_q[x, y] / (y^2 - f(x))$$

der holomorphen Funktionen auf $C \setminus \{P_\infty\}$, gilt

$$\mathrm{Jac}(C)(\mathbb{F}_q) \simeq \mathrm{Cl}(\mathcal{O}),$$

wobei $\mathrm{Cl}(\mathcal{O})$ die Idealklassengruppe des Ringen $\mathcal{O}$ ist.

Bemerkung 2.2.1. Für generische nicht-hyperelliptische Kurven ist die Isomorphie zwischen Idealklassengruppe und Divisorenklassengruppe nicht erfüllt. Allerdings gilt sie noch für die Klasse der sogenannten C_{ab}-Kurven (siehe [66]), (a, b teilerfremd)

$$C_{ab}: \; y^a + \sum_{i=1}^{a-1} f_i(x) y^i + f_0(x) = 0,$$

vom Geschlecht

$$g = (a-1)(b-1)/2$$

mit $f_i(x) \in k\,[x]$, $\deg(f_0) = b$ und $a \deg(f_i(x)) + bi < ab$ für $i = 1, \ldots, a-1$.

Für imaginär quadratische hyperelliptische Kurven hat Mumford in seiner Arbeit [70] die Beziehung zwischen Idealklassengruppe und Divisorenklassengruppe explizit gegeben:

Satz 2.2.7 (Mumford-Darstellung). Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve mit affinem Modell $y^2 + h(x)y = f(x)$, wobei $f, h \in \mathbb{F}_q\,[x]\,,\ \deg(f) = 2g+1$ und $\deg(h) \leq g$. Jede nicht-triviale Idealklasse über $\mathbb{F}_{q^n}$ besitzt einen eindeutigen Repräsentanten, der durch Polynome $u(x)$ und $y - v(x)$ erzeugt wird, so dass gilt:

- $u, v \in \mathbb{F}_{q^n}\,[x]$ mit $\deg(v) < \deg(u) \leq g$,
- u ist normiert,
- $u | v^2 + vh - f$.

Sei $P_i = (x_i, y_i)$ und $D = \sum_{i=1}^r n_i P_i - rP_\infty$ mit $P_i \neq P_\infty,\ P_i \neq \tau P_j$ für $i \neq j$ und $\sum_{i=1}^r n_i \leq g$. Die der Divisorenklasse $[D]$ entsprechende Idealklasse wird durch das Polynom $u = \prod_{i=1}^r (x - x_i)^{n_i}$ und das Polynom v mit

$$\left(\frac{d}{dx}\right)^j \left[v(x)^2 + v(x)h(x) - f(x)\right]_{|x=x_i} = 0,\ 0 \leq j \leq n_i - 1,$$

dargestellt.

Das durch $u(x)$ und $y - v(x)$ eindeutig erzeugte Ideal bezeichnen wir im folgenden mit den Koordinaten (u, v). Der zweite Teil des Satzes besagt, dass $u(x_i) = 0$ und $y_i = v(x_i)$ (gezählt mit Vielfachheit) für alle Punkte $P_i = (x_i, y_i)$ des Trägers von D gilt.

Die Addition von Divisorenklassen entspricht genau der Multiplikation von Idealklassen, welche aus zwei Schritten besteht: Komposition und Reduktion. Der Algorithmus von Cantor [10] liefert eine explizite Beschreibung dieser zwei Schritte.

Algorithmus 1 Cantor'sche Komposition.

INPUT: $D_1 = (u_1, v_1)$ und $D_2 = (u_2, v_2)$
OUTPUT: $D = (u, v)$ semi-reduziert mit $D \sim D_1 \oplus D_2$

1. $d_1 = e_1 u_1 + e_2 u_2 \longleftarrow \gcd(u_1, u_2)$ [mit erweiterten Euklid]

2. $d = c_1 d_1 + c_2(v_1 + v_2 + h) \longleftarrow \gcd(d_1, v_1 + v_2 + h)$ [wie in 1]

3. $s_1 \longleftarrow c_1 e_1, s_2 \longleftarrow c_1 e_2, s_3 \longleftarrow c_2$

4. $u \longleftarrow \dfrac{u_1 u_2}{d^2}$

$v \longleftarrow \dfrac{s_1 u_1 v_2 + s_2 u_2 v_1 + s_3(v_1 v_2 + f)}{d} \mod u$

return (u, v)

Algorithmus 2 Cantor'sche Reduktion.

INPUT: $D = (u, v)$ semi-reduziert
OUTPUT: $D' = (u', v')$ reduziert mit $D' \sim D$

1. $u' \longleftarrow \dfrac{f - vh - v^2}{u}$

$v' \longleftarrow -(h + v) \mod u'$

2. **If** $\deg(u') > g$ **then** $u \longleftarrow u', v \longleftarrow v'$ and **goto 1**

3. Normiere u'

return (u', v')

Stein [90] und Enge [21] haben die Komplexität des Algorithmus von Cantor untersucht und bewiesen, dass eine generische Addition (bzw. Verdopplung) $17g^2 + \mathcal{O}(g)$ (bzw. $16g^2 + \mathcal{O}(g)$) Operationen im Grundkörper $\mathbb{F}_q$ kostet. Um bessere

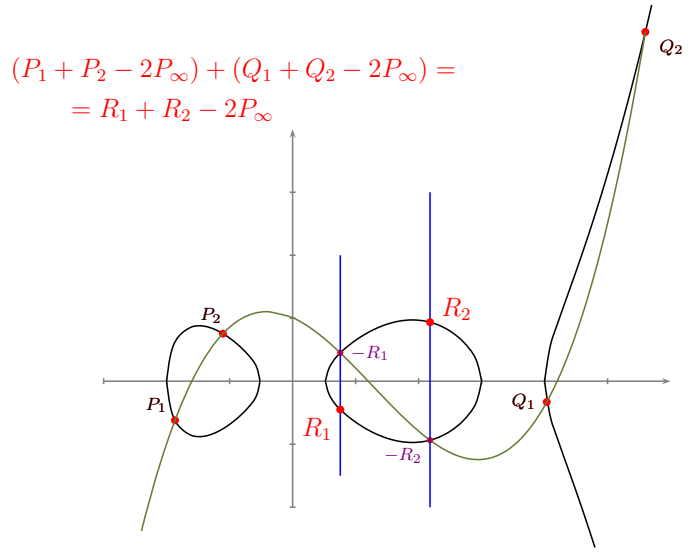


Abbildung 2.1: Addition auf der Jacobischen hyperelliptischer Kurven, $g = 2$

Geschwindigkeit für die Arithmetik auf der Jacobischen zu haben, ist es sinnvoll den Cantor'schen Algorithmus durch explizite Formeln zu ersetzen. Inzwischen wurden für hyperelliptischen Kurven vom Geschlecht $g \leq 3$ explizite Formeln entwickelt, die HECC zu einer der attraktivsten Alternativen zum RSA machen [58, 61, 54, 30, 72, 39].

2.2.7 Linearsysteme und kanonische Einbettungen

Sei C/k eine vollständige glatte absolut irreduzible Kurve und $D \in \mathrm{Div}(C)$ ein Divisor. Als **vollständiges Linearsystem** von D bezeichnen wir die Menge

$$|D| := \{D' \in \mathrm{Div}(C) : \ D' \geq 0, \ D' \sim D\} = \{D + (f) : f \in \mathcal{L}(D)\}$$

aller effektiven Divisoren, die linear äquivalent zu D sind. Zwei Elemente $D+(f)$ und $D+(g)$ aus $|D|$ sind genau dann gleich, wenn es eine Konstante $\lambda \in k^*$ mit $f = \lambda g$ gibt. Also gilt

$$|D| \simeq \mathcal{L}(D)/k^* = \mathbb{P}(\mathcal{L}(D)).$$

Da $|D|$ in Bijektion zum projektiven Raum $\mathbb{P}(\mathcal{L}(D))$ steht, können wir $|D|$ mit der Struktur eines projektiven Raumes versehen: seine Dimension ist dann

$$\dim |D| = l(D) - 1.$$

Ein Punkt P_0 von C heißt **Basispunkt** des Linearsystems $|D|$, wenn

$$P_0 \in \bigcap_{D' \in |D|} \mathrm{Supp}(D').$$

Das Linearsystem $|D|$ heißt **basispunktfrei**, falls

$$\bigcap_{D' \in |D|} \mathrm{Supp}(D') = \emptyset.$$

Man sieht leicht, dass eine Kurve C vom Geschlecht $g \geq 2$ genau dann hyperelliptisch ist, wenn es ein basispunktfreies Linearsystem $|D|$ mit $\deg(D) = 2$ und $\dim|D| = 1$ gibt.
Falls $|D|$ basispunktfrei ist, so definiert die Abbildung

$$i_D : \ C \longrightarrow \mathbb{P}(\mathcal{L}(D))^*, \quad P \longmapsto (s_0(P) : \cdots : s_N(P))$$

einen Morphismus, wobei $\{s_0, \ldots, s_N\}$ eine $\bar{k}$-Basis von $\mathcal{L}(D)$ ist.

Im allgemeinen ist dieser Morphismus nicht injektiv:

Definition 2.2.5. Das basispunktfreie Linearsystem heißt **sehr ample**, falls der Morphismus i_D eine Einbettung von C definiert. Das Bild $i_D(C)$ ist dann eine Kurve vom Grad $\deg(D)$ in $\mathbb{P}^N(\bar{k})$.

Proposition 2.2.3. ([40, IV, 3.1])

(i) Das Linearsystem $|D|$ ist genau dann basispunktfrei, wenn für alle Punkte $P \in C$ gilt
$$\dim|D - P| = \dim|D| - 1$$

(ii) Das Linearsystem $|D|$ ist genau dann sehr ample, wenn für alle Punkte $P, Q \in C$ gilt
$$\dim|D - P - Q| = \dim|D| - 2$$

Lemma 2.2.4. Ist K_C ein kanonischer Divisor einer Kurve C vom Geschlecht $g \geq 1$, so ist das Linearsystem $|K_C|$ basispunktfrei.

Beweis. Falls $g = 1$, so ist $K_C \sim 0$ und somit $|K_C| = 0$ und wir sind fertig.
Sei nun $g \geq 2$. Das Linearsystem $|K_C|$ ist genau dann basispunktfrei, wenn

$$\dim|K_C - P| = \dim|K_C| - 1$$

für alle Punkte $P \in C$ erfüllt ist. Nach dem Satz von Riemann-Roch gilt

$$\dim|P| = \dim|K_C - P| + 1 + 1 - g.$$

Aus

$$\dim|K_C| = g - 1,$$

folgt unmittelbar

$$\dim |K_C - P| = \dim |K_C| - 1 + \dim |P|.$$

Daher ist $|K_C|$ basispunktfrei genau dann wenn $\dim |P| = 0$ für alle $P \in C$. Dies trifft genau dann zu, wenn die Kurve nicht rational ist, d.h. für $g \neq 0$. □

Satz 2.2.8. Eine Kurve C vom Geschlecht $g \geq 3$ ist genau dann nicht-hyperelliptisch, wenn $|K_C|$ sehr ample ist. In diesem Fall bezeichnen wir die **kanonische Einbettung** der Kurve C in $\mathbb{P}\left(\mathcal{L}(K_C)\right)^*$ mit i_{K_C}.

Beweis. Das Linearsystem $|K_C|$ ist genau dann sehr ample, wenn

$$\dim |K_C - P - Q| = \dim |K_C| - 2$$

für alle Punkte $P, Q \in C$ gilt. Nach dem Satz von Riemann-Roch gilt

$$\dim |P + Q| - \dim |K_C - P - Q| = 2 + 1 - g = 3 - g = 2 - \dim |K_C|.$$

Folglich ist $|K_C|$ genau dann sehr ample, wenn $\dim |P+Q| = 0$ für alle $P, Q \in C$. Dies ist aber genau dann der Fall, wenn die Kurve C nicht-hyperelliptisch ist. □

Ist C hyperelliptisch vom Geschlecht g, so ist das Bild von C unter dem kanonischen Morphismus i_{K_C} eine normale rationale Kurve C_0 vom Grad $g-1$, und der Grad des Morphismus $i_{K_C} : C \longrightarrow C_0$ ist 2 (siehe [65]). Ist C nicht-hyperelliptisch, so ist $i_{K_C}(C)$ eine Kurve in $\mathbb{P}^{g-1}$ vom Grad $2g - 2$.

2.2.8 Wendepunkte algebraischer Kurven

In diesem Abschnitt beschreiben wir eine Methode zur Berechnung der Wendepunkte algebraischer Kurven vom Grad n über Körpern mit $\mathrm{char}(k)|2(n-1)$. Als interessante Folgerung zeigen wir, dass die Wendepunkte einer ebenen Quartik C über $\mathbb{F}_{3^n}$ genau den Schnittpunkten von C mit einer Quadrik h_C entsprechen.

Sei k ein algebraisch abgeschlossener Körper der Charakteristik $p \geq 0$, und $f \in k\left[x_1, x_2, x_3\right]$ ein homogenes Polynom vom Grad n. Mit f_i und f_{ij} bezeichnen wir die partiellen Ableitungen

$$f_i := \frac{\partial f}{\partial x_i},\ f_{ij} := \frac{\partial f_i}{\partial x_j} = \frac{\partial^2 f}{\partial x_j \partial x_i}.$$

Definition 2.2.6. Die **Hessematrix** von f ist die Matrix $(f_{ij})_{i,j}$. Ihre Determinante $H(f)$ heißt die **Hessesche** von f.

Lemma 2.2.5. Ist $g \in \mathrm{GL}_3(k)$ eine lineare Transformation, so gilt

$$H(f \circ g^{-1}) = (\det g)^2 H(f) \circ g^{-1}.$$

Beweis. Der Beweis ist offensichtlich unter Verwendung der Kettenregel. □

Lemma 2.2.6. $x_1^2 H(f) = \begin{vmatrix} n(n-1)f & (n-1)f_2 & (n-1)f_3 \\ (n-1)f_2 & f_{22} & f_{23} \\ (n-1)f_3 & f_{23} & f_{33} \end{vmatrix}$

Beweis. Wegen der Eulerschen Formel (siehe z.B. [71]) gilt

$$\sum_{i=1}^{3} x_i f_{ij} = (n-1) f_j \text{ für } j = 1, 2, 3$$

und nach Addition der x_i-fachen der i-ten Zeile (für $i = 2, 3$) zur ersten Zeile der Matrix

$$x_1 H(f) = \begin{vmatrix} x_1 f_{11} & x_1 f_{12} & x_1 f_{13} \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{vmatrix},$$

erhalten wir

$$x_1 H(f) = (n-1) \begin{vmatrix} f_1 & f_2 & f_3 \\ f_{21} & f_{22} & f_{23} \\ f_{31} & f_{32} & f_{33} \end{vmatrix}.$$

Wieder unter Verwendung der Eulerschen Formel

$$x_1 f_1 + x_2 f_2 + x_3 f_3 = n \cdot f$$

und Addition der x_j-fachen der j-ten Spalte (für $j = 2, 3$) zur ersten Spalte der obigen Matrix, erhält man

$$x_1^2 H(f) = \begin{vmatrix} n(n-1)f & (n-1)f_2 & (n-1)f_3 \\ (n-1)f_2 & f_{22} & f_{23} \\ (n-1)f_3 & f_{23} & f_{33} \end{vmatrix}$$

□

Definition 2.2.7. Sei C/k eine ebene Kurve. Sei P ein nicht-singulärer Punkt von C und t_P die Tangente zu C bei P. Der Punkt P heißt **Wendepunkt** von C, falls die Schnittvielfachheit $I(C, t_P, P)$ von C mit der Tangente t_P bei P größer oder gleich 3 ist.

Ist $n \geq 3$ und die Kurve C/k gegeben durch die Gleichung $f = 0$ und $P = (p_1 : p_2 : p_3)$ ein nicht-singulärer Punkt von C, so gibt es eine lineare Transformation g, die P auf $(1 : 0 : 0)$ und seine Tangente auf $x_3 = 0$ abbildet. In affinen Koordinaten gilt

$$f \circ g^{-1} = x_3 + rx_2^2 + sx_2x_3 + tx_3^2 + R(x_2, x_3), \quad r, s, t \in \bar{k} \tag{2.1}$$

wobei R nur aus Monomen vom Grad ≥ 3 besteht. Der Punkt P ist genau dann ein Wendepunkt von C, wenn $r = 0$ gilt.

Proposition 2.2.4. Sei $p \neq 2$ und $n - 1 \not\equiv 0 \mod p$. Ein Punkt P von C ist genau dann ein Wendepunkt, wenn gilt:

$$H(f)(P) = 0.$$

Insbesondere gilt: Hat C einen nicht-singulären Punkt, der kein Wendepunkt ist, so hat C eine endliche Anzahl von Wendepunkten.

Beweis. Sei o.B.d.A die x_1-Koordinate von P verschieden von 0. Wegen Lemma 2.2.5 gilt:

$$(x_1^2 H(f) \circ g^{-1})(g(P)) = (\det g)^{-2}(x_1^2 H(f \circ g^{-1}))(g(P)).$$

Wegen der Gestalt von $f \circ g^{-1}$ in (2.1) und Lemma 2.2.6, folgt

$$(x_1^2 H(f))(P) = -(\det g)^{-2} 2(n-1)^2 r.$$

Also $H(f)(P) = 0$ genau dann, wenn $r = 0$ (d.h. P ist ein Wendepunkt). □

Ist C vom Grad n und $\mathrm{char}(k) = 0$, so ist wohlbekannt, dass die Hessesche den Grad $3(n-2)$ hat. In diesem Fall gibt es genau $3n(n-2)$ Wendepunkte. Ist aber $\mathrm{char}(k) \neq 0$, so können seltsame Verhalten auftreten: es könnte z.B. Kurven geben, in der alle nicht-singulären Punkte Wendepunkte sind.

Beispiel 2.2.1. Sei C/k die durch

$$f(x, y, z) := x^p + x^{p-1}y + z^p,$$

definierte Kurve über einem Körper der Charakteristik $p \neq 2$.
Dann ist $\partial f(x, y, z)/\partial z = 0$ und somit $H(f) = 0$. Da $p - 1 \not\equiv 0 \mod p$, können wir wegen Proposition 2.2.4 folgern, dass jeder Punkt von C ein Wendepunkt ist. Solche Kurven, in der die nicht-singulären Punkte den Wendepunkten entsprechen, bezeichnen wir als **eigenartige** Kurve.

Ab jetzt betrachten wir unter anderem den Fall $\mathrm{char}(k) \mid 2(n-1)$. Sei dazu k ein algebraisch abgeschlossener Körper der Charakteristik $p > 0$. Sei K ein vollständiger lokaler Körper der Charakteristik 0 mit Ganzheitsring $\mathcal{O}$ und maximalem Ideal $\mathcal{M}$, so dass $\mathcal{O}/\mathcal{M} \simeq k$.

Proposition 2.2.5. Sei $\tilde{f} \in k[x_1, x_2, x_3]$ ein homogenes Polynom vom Grad n. Sei $\tilde{C} = V(\tilde{f})$ und $C/\mathcal{O}$ ein Modell von $\tilde{C}$, welches durch ein Polynom $f \in \mathcal{O}[x_1, x_2, x_3]$ definiert ist. Dann ist das Polynom

$$G = \frac{x_1^2 H(f) - n(n-1) f (f_{22} f_{33} - f_{23}^2)}{2(n-1)^2}$$

in $\mathcal{O}[x_1, x_2, x_3]$. Wir bezeichnen die Reduktion von G modulo $\mathcal{M}$ mit $\tilde{G}$, wobei $\mathcal{M}$ das maximale Ideal von $\mathcal{O}$ ist. Ein nicht-singulärer Punkt $\tilde{P} = (\tilde{p}_1 : \tilde{p}_2 : \tilde{p}_3) \in \tilde{C}$ mit $\tilde{p}_1 \neq 0$ ist genau dann ein Wendepunkt, wenn $\tilde{G}(\tilde{P}) = 0$.

Beweis. Zuerst beweisen wir, dass G in $\mathcal{O}[x_1, x_2, x_3]$ liegt. Wegen Lemma 2.2.6 gilt:

$$x_1^2 H(f) - n(n-1) f (f_{22} f_{33} - f_{23}^2) = (n-1)^2 (2 f_2 f_3 f_{23} - f_2^2 f_{33} - f_3^2 f_{22}).$$

Also teilt $2(n-1)^2$ den Ausdruck $x_1^2 H(f) - n(n-1) f (f_{22} f_{33} - f_{23}^2)$.
Sei $\tilde{P}$ ein nicht-singulärer Punkt von $\tilde{C}$ mit $\tilde{p}_1 \neq 0$. Da $\tilde{P}$ nicht-singulär ist, gibt es ein $P = (p_1 : p_2 : p_3) \in C(\mathcal{O})$, das $\tilde{P}$ liftet und $p_1 \notin \mathcal{M}$. Sei $g \in \mathrm{GL}_3(\mathcal{O})$ eine lineare Transformation, die den Punkt P auf $(1:0:0)$ und dessen Tangente auf $x_3 = 0$ abbildet. Die Reduktion dieses Punktes ist genau dann ein Wendepunkt, wenn das entsprechende r aus (2.1) ein Element von $\mathcal{M}$ ist. Nun gilt $G(P) = ur$ mit $u \in \mathcal{O}^*$ durch Anwendung von Proposition 2.2.4. Also ist $\tilde{P}$ ein Wendepunkt genau dann, wenn $\tilde{G}(\tilde{P}) = 0$. □

Ab jetzt betrachten wir nur ebene **Quartiken**, d.h. Kurven vom Grad $n = 4$.

Proposition 2.2.6. [43] C/k ist genau dann eine eigenartige ebene Quartik, wenn eine der folgenden Bedingungen erfüllt ist:

(i) $\mathrm{char}(k) = 2$ und C ist isomorph zu einer singulären Kurve der Gestalt

$$y^4 = x^3 z + a x^2 z^2 + x z^3, \ a \in k$$

mit einzigen singulären Punkt $(1 : \sqrt[4]{a} : 1)$. Außerdem ist die Schnittvielfachheit $I(C, t_P; P)$ von C mit der Tangente t_P an einem generischen Punkt P gleich 4. M.a.W., die generischen Punkte von C entsprechen den **Hyperwendepunkten** von C.

(ii) $\mathrm{char}(k) = 3$ und C ist isomorph zur **Klein Quartik**

$$x^3y + y^3z + z^3x = 0.$$

Proposition 2.2.7. Sei $\tilde{C}/k$ gegeben durch $\tilde{f} = 0$ eine glatte ebene Quartik über einem Körper k der Charakteristik 3. Ist $\tilde{C}$ keine eigenartige Kurve, so entsprechen die Wendepunkte von $\tilde{C}$ genau den Schnittpunkten von $\tilde{C}$ mit einer über k definierten Quadrik $h_{\tilde{C}}$.

Beweis. Sei $\tilde{P} = (\tilde{p_1} : \tilde{p_2} : \tilde{p_3}) \in \tilde{C}(\bar{k})$ ein Wendepunkt von $\tilde{C}$. Wir können o.B.d.A annehmen, dass $\tilde{p_3} \neq 0$ für alle Wendepunkte von C ist. Seien ferner f, G und $\tilde{G}$ wie in Proposition 2.2.5. Wie im Beweis von Proposition 2.2.5 gilt

$$\begin{aligned} 2\tilde{G} &= 2\tilde{f_1}\tilde{f_2}\tilde{f_{12}} - \tilde{f_1}^2\tilde{f_{22}} - \tilde{f_2}^2\tilde{f_{11}}, \\ &= \tilde{f_1}(\tilde{f_2}\tilde{f_{12}} - \tilde{f_1}\tilde{f_{22}}) + \tilde{f_2}(\tilde{f_1}\tilde{f_{12}} - \tilde{f_2}\tilde{f_{11}}). \end{aligned}$$

Ist nun $\tilde{f}$ gegeben durch

$$\begin{aligned} \tilde{f}(x,y,z) &:= a_{00}y^4 + y^3(a_{10}x + a_{01}z) + y^2(a_{20}x^2 + a_{11}xz + a_{02}z^2) \\ &\quad + y(a_{30}x^3 + a_{21}x^2z + a_{12}xz^2 + a_{03}z^3) \\ &\quad + (a_{40}x^4 + a_{31}x^3z + a_{22}x^2z^2 + a_{13}xz^3 + a_{04}z^4), \end{aligned}$$

so überprüft man leicht durch explizite Berechnungen (z.B. mit MAPLE), dass

$$2\tilde{G} - a_{20}\tilde{f}^2 + \tilde{f}(ax^3 + by^3 + cz^3)z = H_{\tilde{C}} \cdot z^2,$$

mit

$$\begin{aligned} a &:= a_{40}a_{11} + a_{21}a_{30} - 2a_{20}a_{31}, \\ b &:= a_{10}a_{11} + a_{00}a_{21} - 2a_{20}a_{01}, \\ c &:= 2a_{12}^2 + a_{13}a_{11} + a_{20}a_{04} + a_{03}a_{21} + a_{02}a_{22}, \end{aligned}$$

wobei $H_{\tilde{C}}$ ein homogenes Polynom in $k[x,y,z]$ vom Grad 6 ist, in dem nur Terme mit Monomen $x^6, y^6, z^6, x^3y^3, x^3z^3, y^3z^3$ auftreten. Da $x \mapsto x^3$ ein Isomorphismus von $k = \mathbb{F}_{3^n}$ ist, gibt es ein $h_{\tilde{C}} \in k[x,y,z]$ mit $H_{\tilde{C}} = h_{\tilde{C}}^3$. □

Kapitel 3

Arithmetik auf Jacobischen glatter Quartiken

In diesem Kapitel werden wir uns mit der Arithmetik auf Jacobischen nicht-hyperelliptischer Kurven des Geschlechts 3 befassen.

Als erstes werden wir grundlegende Eigenschaften sowie die Invariantentheorie für nicht-hyperelliptische Kurven vom Geschlecht 3 beschreiben.

Wie bei elliptischen und hyperelliptischen Kurven werden wir eine Art *Tangente-Sekante* Methode für die Gruppenoperation auf Jacobischen nicht-hyperelliptischer Kurven vom Geschlecht 3 ableiten: dabei werden *Tangente* sowie *Sekante* durch *Kubik* ersetzt, und es wird eine zusätzliche *Quadrik* zur Berechnung von Inversen eingeführt. Dieser Algorithmus hat nicht nur eine schöne geometrische Beschreibung, sondern liefert den bis dato besten Algorithmus zur Addition auf der Jacobischen einer nicht-hyperelliptischen Kurve vom Geschlecht 3.

3.1 Nicht-hyperelliptische Kurven mit g = 3

Wir werden uns im folgenden mit der Beschreibung nicht-hyperelliptischer Kurven vom Geschlecht 3 beschäftigen.

3.1.1 Glatte Quartiken in $\mathbb{P}^2$

Sei C eine nicht-hyperelliptische Kurve vom Geschlecht 3 und $\{\omega_1, \omega_2, \omega_3\}$ eine Basis von $\Omega^1(C)$. Die kanonische Einbettung i_{K_C} ist bezüglich dieser Basis durch

$$i_{K_C} : C \longrightarrow \mathbb{P}^2, \quad P \longmapsto (\omega_1(P) : \omega_2(P) : \omega_3(P))$$

definiert, dabei ist $\omega(P) := f(P)$ für $\omega = f dt_P$ mit $f, t_P \in k(C)$ und t_P ein lokaler Parameter bei P.
Ist $H = V(a_1x_1 + a_2x_2 + a_3x_3)$ eine Gerade in $\mathbb{P}^2$, so gilt für den *Pullback* $i^*_{K_C}$ von i_{K_C}

$$i^*_{K_C}(i_{K_C}(C) \cdot H) = (a_1\omega_1 + a_2\omega_2 + a_3\omega_3),$$

so dass $i_{K_C}(C)$ eine glatte Quartik ist.

Proposition 3.1.1. ([40, IV, Ex. 3.2]) Sei C eine glatte ebene Quartik über einem Körper k. Dann gilt:

(i) C ist eine Kurve vom Geschlecht 3.

(ii) Die effektiven kanonischen Divisoren von C sind genau die Schnittdivisoren $(C \cdot l)$ mit Geraden l.

(iii) C ist nicht-hyperelliptisch.

Als Folge der obigen Resultate erhält man den folgenden:

Satz 3.1.1. Sei C eine nicht-hyperelliptische Kurve vom Geschlecht 3. Das Bild von C unter der kanonischen Einbettung ist eine glatte Quartik, und umgekehrt ist jede glatte Quartik das Bild der kanonischen Einbettung einer nicht-hyperelliptischen Kurve vom Geschlecht 3.

Eine interessante Klasse von glatten Quartiken unter den C_{34}-Kurven bilden die Picard-Kurven: eine **Picard Kurve** C/k über einem Körper k mit $\mathrm{char}(k) \neq 3$ ist eine nicht-hyperelliptische Kurve vom Geschlecht 3 mit (affinem) Modell

$$y^3 = f(x),$$

wobei $f(x) \in k[x]$ ein normiertes Polynom vom Grad 4 ist, das nur einfache Nullstellen in $\bar{k}$ besitzt.

Für den Rest dieser Arbeit ist immer eine glatte ebene Quartik gemeint, wenn von einer nicht-hyperelliptischen Kurve vom Geschlecht 3 die Rede ist.

Lemma 3.1.1. Sei C eine glatte Quartik in $\mathbb{P}^2$. Für die Dimension von $\mathcal{L}$-Räumen positiver Divisoren gilt:

$$\begin{aligned}
l(P+Q) &= 1 \text{ für alle Punkte } P, Q \in C, \\
l(P+Q+R) &= \begin{cases} 2 & , \text{ falls } P,Q,R \text{ kollinear sind} \\ 1 & , \text{ sonst} \end{cases} \\
l(P+Q+R+S) &= \begin{cases} 3 & , \text{ falls } P,Q,R,S \text{ kollinear sind} \\ 2 & , \text{ sonst} \end{cases} \\
l(D) &= \deg(D) - 2 \text{ für } \deg(D) \geq 5.
\end{aligned}$$

Beweis. Sei K_C ein kanonischer Divisor von C.

(i) Die Gerade l durch P und Q schneidet C in zwei weiteren Punkten R und S. Da C nicht-hyperelliptisch ist, ist $K_C \sim P+Q+R+S$ sehr ample, also gilt

$$l(P+Q) = l(P+Q+R+S-(R+S)) = l(K_C-(R+S)) = l(K_C)-2 = 1.$$

(ii) Aus

$$l(P+Q+R) - l(K_C-(P+Q+R)) = \deg(P+Q+R)+1-3 = 1$$

und nach dem Satz vom Clifford folgt

$$l(K_C-(P+Q+R)) \in \{0,1\}.$$

Dabei ist $l(K_C-(P+Q+R)) = 1$ genau dann, wenn es einen Punkt $S \in C$ mit $K_C-(P+Q+R) \sim S$ gibt, also wenn P,Q,R kollinear sind.

(iii) wie in (iii):

$$l(P+Q+R+S)-l(K_C-(P+Q+R+S)) = \deg(P+Q+R+S)+1-3 = 2$$

und nach dem Satz vom Clifford folgt

$$l(K_C-(P+Q+R+S)) \in \{0,1\}.$$

Dabei ist $l(K_C-(P+Q+R+S)) = 1$ genau dann der Fall, wenn $K_C-(P+Q+R+S) \sim 0$, also wenn P,Q,R,S kollinear sind.

(iv) Für $\deg(D) \geq 5$ ist $l(K_C-D) = 0$, und aus dem Satz von Riemann-Roch folgt $l(D) = \deg(D)+1-3 = \deg(D)-2$.

□

Definition 3.1.1. Eine **Bitangente** von C/k ist eine Gerade l mit einem Schnittdivisor $(l \cdot C) = 2P+2Q$ für (nicht notwendigerweise verschiedene) Punkte $P,Q \in C$. Ist ferner $P = Q$, so heißt P **Hyperwendepunkt** von C.

Besitzt C/k einen Hyperwendepunkt P_∞, so ist P_∞ bereits über k definiert.

Im allgemeinen hat eine glatte Quartik keinen Hyperwendepunkt, da der Modulraum von glatten ebenen Quartiken mit mindestens einem Hyperwendepunkt die Kodimension 1 im Modulraum der allgemeinen Quartiken hat. Wendepunkte

sowie Hyperwendepunkte einer glatten ebenen Quartik C entsprechen genau den Weierstrass-Punkten erster und zweiter Ordnung.

Sei l_0 eine Bitangente mit $(l_0 \cdot C) = 2P_0 + 2Q_0$. Ist l eine andere Bitangente und P, Q Punkte mit $(l \cdot C) = 2P + 2Q$, so gilt

$$P + Q - (P_0 + Q_0) \in \mathrm{Jac}(C)[2].$$

Proposition 3.1.2. Sei C eine glatte Quartik über einem algebraisch abgeschlossenen Körper $\bar{k}$ der Charakteristik $p \geq 0$.

(i) Sei $p \neq 2$. Dann besitzt C genau 28 Bitangenten.

(ii) Sei $p = 2$. Ist der 2-Rang von $\mathrm{Jac}(C)$ gleich 0 (bzw. $1, 2, 3$), so besitzt C genau 1 (bzw. $2, 4, 7$) Bitangenten.

Satz 3.1.2 ([59])**.** Jede glatte Quartik $C/\mathbb{C}$ ist durch ihre Bitangenten eindeutig rekonstruierbar.

Das in Kapitel 4 vorgestellte Riemann-Modell für glatte Quartiken und die Eindeutigkeitsaussage von Satz 3.1.2 werden ein algorithmisches Rekonstruktionsverfahren für Quartiken, deren Bitangenten gegeben sind, liefern.

3.1.2 Dixmier-Invarianten glatter Quartiken in $\mathbb{P}^2$

In diesem Abschnitt führen wir Invariantensysteme für glatte Quartiken ein. Falls nicht anders erwähnt sei im folgenden $k = \mathbb{C}$.

Sei V die Menge der **ternären** Quartiken, d.h. die Menge der homogenen Polynome vom Grad 4 in drei Variablen mit komplexen Koeffizienten. V bildet einen $\mathbb{C}$-Vektorraum der Dimension 15. Sei $\mathbb{C}[V]$ die Algebra der komplexen Polynome in V und $\mathbb{C}[V]_n$ die Menge der homogenen Elemente vom Grad n in $\mathbb{C}[V]$. Die Algebra $\mathbb{C}[V] = \bigoplus_{n \geq 0} \mathbb{C}[V]_n$ ist eine graduierte Algebra, auf der die Gruppe $\mathrm{SL}_3(\mathbb{C})$ auf natürliche Weise operiert. $\mathbb{C}[V]_n$ ist invariant unter der Operation von $\mathrm{SL}_3(\mathbb{C})$. Sei $\mathfrak{A}$ die Menge der Elemente in $\mathbb{C}[V]$, die unter $\mathrm{SL}_3(\mathbb{C})$ invariant sind. Die Menge $\mathfrak{A}$ ist eine graduierte Unteralgebra von $\mathbb{C}[V]$, die Algebra der (projektiven) **Invarianten** ebener Quartiken. Die Algebra $\mathfrak{A}$ besitzt ein System von Invarianten $I_3, I_6, I_9, I_{12}, I_{15}, I_{18}, I_{27}$ der Ordnungen $3, 6, 9, 12, 15, 18, 27$.

Die Invarianten I_3 und I_6 einer Quartik der Form

$$\begin{aligned} g(x,y,z) \;:=\; & a_1x^4 + 4a_2x^3y + 6a_3x^2y^2 + 4a_4xy^3 + a_5y^4 + 4a_6x^3z + 12a_7x^2yz \\ & + 12a_8xy^2z + 4a_9y^3z + 6a_{10}x^2z^2 + 12a_{11}xyz^2 + 6a_{12}y^2z^2 \\ & + 4a_{13}xz^3 + 4a_{14}yz^3 + a_{15}z^4 \end{aligned}$$

lassen sich explizit via

$$\begin{aligned} I_3(g) \;:=\; & a_1a_5a_{15} + 3(a_1a_{12}^2 + a_5a_{10}^2 + a_{15}a_3^2) + 4(a_2a_9a_{13} + a_6a_4a_{14}) \\ & -4(a_1a_9a_{14} + a_5a_6a_{13} + a_{15}a_2a_4) + 6a_3a_{10}a_{12} - 12a_7a_8a_{11} \\ & -12(a_2a_{11}a_{12} + a_6a_8a_{12} + a_4a_{11}a_{10} + a_9a_7a_{10} + a_{13}a_8a_3 + a_{14}a_7a_3) \\ & +12(a_7a_4a_{13} + a_8a_{14}a_2 + a_{11}a_6a_9) + 12(a_3a_{11}^2 + a_{10}a_8^2 + a_{12}a_7^2) \end{aligned}$$

und

$$I_6(g) \;:=\; \det \begin{bmatrix} a_1 & a_3 & a_{10} & a_7 & a_6 & a_2 \\ a_3 & a_5 & a_{12} & a_9 & a_8 & a_4 \\ a_{10} & a_{12} & a_{15} & a_{14} & a_{13} & a_{11} \\ a_7 & a_9 & a_{14} & a_{12} & a_{11} & a_8 \\ a_6 & a_8 & a_{13} & a_{11} & a_{10} & a_7 \\ a_2 & a_4 & a_{11} & a_8 & a_7 & a_3 \end{bmatrix}$$

berechnen.

In [18] gibt Dixmier ein algorithmisches Verfahren zur Berechnung der restlichen Invarianten $I_9, I_{12}, I_{15}, I_{18}, I_{27}$. Eine Beschreibung durch explizite Formeln ist jedoch schwierig, da die auftretende Formeln sehr umfangreich sind.

Eine ebene Quartik $C : g(x, y, z) = 0$ ist genau dann vom Geschlecht 3, wenn ihre **Diskriminante** $I_{27} \neq 0$ ist (siehe [18]). Für eine glatte ternäre Quartik lassen sich mit Hilfe der Invarianten $I_3, I_6, I_9, I_{12}, I_{15}, I_{18}, I_{27}$ die absolute Invarianten

$$i_1 = \tfrac{I_3^9}{I_{27}}, \quad i_2 = \tfrac{I_3^7 I_6}{I_{27}}, \quad i_3 = \tfrac{I_3^6 I_9}{I_{27}}, \quad i_4 = \tfrac{I_3^5 I_{12}}{I_{27}}, \quad i_5 = \tfrac{I_3^4 I_{15}}{I_{27}}, \quad i_6 = \tfrac{I_3^3 I_{18}}{I_{27}}$$

zuordnen. Da die I_j unter $\mathrm{SL}_3(\mathbb{C})$ invariant sind, sind die i_j unter $\mathrm{GL}_3(\mathbb{C})$ invariant, genauer gesagt, haben wir das folgende:

Lemma 3.1.2. Seien C und C' zwei ternäre Quartiken vom Geschlecht 3. Sind C und C' isomorph, so gelten für die Invarianten:

$$i_j(C) = i_j(C') \qquad \text{für} \qquad j = 1, \ldots, 6.$$

Beweis. Sei $C' = C^\alpha$ mit $\alpha \in \mathrm{GL}_3(\mathbb{C})$ und $D := \det(\alpha) \neq 0$. Nach [82] gelten für die Invarianten I_j und I'_j von C und C'

$$I'_j = (D^4)^{\frac{j}{3}} \cdot I_j$$

für $j = 3, 6, 9, 12, 15, 18, 27$. Durch Anwendung der Definition der i_j folgt die Behauptung. □

Bemerkung 3.1.1.

(i) Ob die Umkehrung von Lemma 3.1.2 richtig ist, ist bis heute noch offen.

(ii) Die Dixmier-Invarianten $i_1, \cdots, i_6$ lassen sich auch auf den Fall von Körpern der Charakteristik $p \neq 2, 3$ verallgemeinern.

3.2 Arithmetik auf Jacobischen glatter Quartiken

Die in diesem Abschnitt erzielten Ergebnisse sind in Zusammenarbeit mit S. Flon und C. Ritzenthaler [24, 25] zustandegekommen.

3.2.1 Geometrische Beschreibung

Wenn nicht anders vermerkt, ist C/k eine glatte ebene Quartik und K_C ein kanonischer Divisor von C.

Wir bezeichnen mit $(*)$ die folgende Eigenschaft :

Es gibt eine k-rationale Gerade l^∞, welche C in vier k-rationalen Punkten (mit Multiplizität gezählt) $P_1^\infty, P_2^\infty, P_3^\infty, P_4^\infty$ schneidet.

Für die Gerade l^∞ gibt es fünf verschiedene Möglichkeiten die Quartik zu schneiden:

(i) die vier Punkte sind paarweise verschieden,

(ii) $P_1^\infty = P_2^\infty$, d.h. l^∞ ist Tangente an C im Punkt P_1^∞,

(iii) $P_1^\infty = P_2^\infty = P_4^\infty$. Der Punkt P_1^∞ ist in diesem Fall ein Wendepunkt von C,

(iv) $P_1^\infty = P_2^\infty$ und $P_3^\infty = P_4^\infty$. Die Gerade l^∞ ist eine Bitangente von C,

(v) $P_1^\infty = P_2^\infty = P_3^\infty = P_4^\infty$. Der Punkt P_1^∞ ist in diesem Fall ein Hyperwendepunkt von C.

Die Effizienz unseres Algorithmus wird von der Wahl der Gerade l^∞ abhängen (siehe Abschnitt 3.2.2).

Wir werden im folgenden untersuchen, inwiefern die Bedingung $(*)$ für den endlichen Körper $k = \mathbb{F}_q$ mit $q = p^n$ Elementen erfüllt ist.

Proposition 3.2.1. Die Bedingung $(*)$ ist in den folgenden Fällen erfüllt:

Bedingung an p	**Bedingung an** q	**Bedingung an** $\#C(k)$
1) $p > 2$	$q \geq 10^6$	
2) $p > 2$	$q > 8$	$\#C(k) \geq q - \sqrt{q}/4 + 7/4$
3) $p = 2$	$q > 8$	$\#C(k) \geq q + 3$

Insbesondere gibt es für große q (z.B. für $q \geq 10^6$) immer vier kollineare $\mathbb{F}_q$-rationale Punkte auf einer über $\mathbb{F}_q$ definierten glatten Quartik.

Beweis. Angenommen $(*)$ sei nicht erfüllt. Die Menge der k-rationalen Punkte $\mathcal{K} := C(k)$ von C bildet dann einen $\#C(k)$-*Bogen*, d.h. eine Menge von $\#C(k)$ Punkten, für die je drei Punkte nicht kollinear sind. Aus [42] folgt, dass $\#C(k) \leq q + 2$ falls $p = 2$ (woraus die letzte Zeile der Tabelle folgt), und dass $\#C(k) \leq q + 1$ falls p ungerade ist. Ferner gibt es für ungerades p explizite Schranken $m'(2, q)$, so dass jeder r-Bogen mit $r > m'(2, q)$ eine Untermenge der Menge der k-rationalen Punkte einer Quadrik ist (siehe [42, Tab 1.3]). Wäre also $\#C(k) \geq \max(9, m'(2, q) + 1)$, so müsste die Quartik durch diese Punkte eine Quadrik enthalten, was einen Widerspruch zur Irreduzibilität der Quartik darstellt. Die zweite Zeile der Tabelle in der Proposition folgt sofort aus dieser Bemerkung und aus [42, Tab 1.3].
Nun untersuchen wir die erste Zeile der Tabelle, wo keine Bedingung an $\#C(k)$ angegeben ist. Wir können $\#C(k) \leq m'(2, q)$ annehmen. Aus $q \geq 10^6$, folgt

$$(3q + 5)/4 < \#C(k) \leq m'(2, q)$$

(die erste Ungleichung folgt aus der Hasse-Weil Schranke und ist bereits für $q > 24^2$ erfüllt).
Im folgenden werden wir Ergebnisse sowie Bezeichnungen aus [94] verwenden. In [94] wird zu einem beliebigen Bogen $\mathcal{K}$ eine ebene Kurve $\mathcal{E}$ in der dualen Ebene assoziiert, welche die *Hülle* der 1-Sekanten (die rationalen Geraden, welche $\mathcal{K}$ in einem Punkt treffen) von $\mathcal{K}$ ist. Da $(*)$ nicht erfüllt ist, sind die Tangenten von C an den Punkten von $\mathcal{K}$ 1-Sekanten. Mit dem Satz von Bézout ist die duale Kurve C^* eine irreduzible Komponente von $\mathcal{E}$. Sei P_0 ein Punkt von $C(k)$. Da $(*)$ nicht erfüllt ist, ist P_0 weder auf einer Bitangente noch ein Wendepunkt. Sei l_0 die Tangente an C bei P_0. Wegen den Eigenschaften der dualen Kurve ist der Punkt $l_0^* \in C^*$ ein nicht-singulärer rationaler Punkt. Ferner folgt mit Hilfe von [94, Th. 5.2.(3)], dass $i(\mathcal{E}, P_0^*; l_0^*) = 2 = i(C^*, P_0^*; l_0^*)$ gilt. Also ist C^* keine mehrfache Komponente von $\mathcal{E}$. Ebenso ist der Punkt l_0^* ein *spezieller Punkt,* und C^* ist

eine zu l_0^* assoziierte *irreduzible Hülle.* Mit den Bezeichnungen von [94, Sec. 5.2] folgt $\nu_4 \leq 2\deg(C^*)$; dabei ist ν_4 die *vierte positive $\mathbb{F}_q$-Frobenius Ordnung* einer *linearen Reihe*, und deshalb $\nu_4 \leq 24$ (der Grad der dualen Kurve einer nichtsingulären Kurve vom Grad n ist $\leq n(n-1)$, siehe [43]). Nun können wir [94, Prop. 5.11] anwenden:

$$\#C(k) \leq \min\left(q - \frac{1}{4}\nu_4 + \frac{7}{4},\ \frac{28+4\nu_4}{29+4\nu_4}q + \frac{32+2\nu_4}{29+4\nu_4}\right).$$

Dies führt für $q \geq 10^6$ zu $\#C(k) < q+1-6\sqrt{q}$, ein Widerspruch zur Hasse-Weil Schranke. □

Bemerkung 3.2.1. Die Abschätzungen von Proposition 3.2.1, insbesondere die für $p = 2$, können noch verbessert werden (siehe [42]; man beachte, dass ein *Hyperoval* eine *parametrische* Kurve ist). Ebenso ist es auch möglich, unsere Überlegungen auf den Fall von Körpern der Charakteristik 2 zu erweitern.

Für den Rest dieses Abschnittes setzen wir stets voraus, dass die Bedingung $(*)$ erfüllt ist.

Sei nun $D_i^\infty := \sum_{k=1}^{i} P_k^\infty$, für $i = 1, 2, 3$.

Satz 3.2.1. Zu $D \in \mathrm{Div}_k^0(C)^*$ existiert ein eindeutiger effektiver Divisor $E \in \mathrm{Div}_k(C)$ minimalen Grades $m \in \{1,2,3\}$, so dass $D \sim E - D_m^\infty$. Der reduzierte Divisor E gehört zu genau einer der folgenden Klassen von Divisoren:

(i) $E = P_1 + P_2 + P_3$ mit $l(P_1+P_2+P_3) = 1$ und $P_i \neq P_3^\infty$,

(ii) $E = P_1 + P_2$ mit $P_i \neq P_2^\infty$,

(iii) $E = P_1$ mit $P_1 \neq P_1^\infty$.

Beweis. Der Übersichtlichkeitshalber werden wir uns auf den Sonderfall $P_1^\infty = P_2^\infty = P_3^\infty$ beschränken. Ein vollständiger Beweis würde eine sehr große Anzahl von Fallunterscheidungen erfordern.
Sei $D \in \mathrm{Div}_k^0(C)^*$. Nach Lemma 2.2.2 gibt es Punkte P_1, P_2, P_3 mit $D \sim P_1 + P_2 + P_3 - 3P_1^\infty$. Ist einer der Punkte P_i gleich P_1^∞, so besitzt D eine Darstellung der Form (ii) oder (iii). Ist $P_i \neq P_1^\infty$ und ist $D \sim Q_1+Q_2+Q_3-3P_1^\infty$ eine andere Darstellung von D, so gibt es eine Funktion $f \in k(C)$ mit $f \in \mathcal{L}(P_1+P_2+P_3)$. Dies ist nur dann möglich wenn $l(P_1+P_2+P_3) > 1$ ist, demzufolge ist die in (i) beschriebene Darstellung eindeutig. Ebenso beweist man, dass der Divisor

$P_1 + P_2 + P_3 - 3P_1^\infty$ mit $l(P_1 + P_2 + P_3) = 1$ keine reduzierte Darstellung der Form (ii) oder (iii) besitzt.
Sei nun $l(P_1 + P_2 + P_3) \geq 2$ mit $P_i \neq P_1^\infty$ für $i = 1, 2, 3$. Nach Lemma 3.1.1 sind die Punkte P_i kollinear. Sei l_1 die Gerade durch die Punkte P_i, und sei R der vierte Schnittpunkt von l_1 mit C. Ist $R = P_4^\infty$, so ist $D \sim P_1 + P_2 + P_3 - 3P_1^\infty = P_1 + P_2 + P_3 + P_4^\infty - (3P_1^\infty + P_4^\infty) = (l_1 \cdot C) - (l^\infty \cdot C) \sim 0$. Für $R \neq P_4^\infty$ betrachten wir die Gerade l_2 durch R und P_1^∞ (bzw. die Tangente l^∞ an P_1^∞ für $P_1^\infty = R$). Seien S, T die weiteren Schnittpunkte von l_2 mit C. In diesem Fall gilt $D \sim P_1 + P_2 + P_3 - 3P_1^\infty = P_1 + P_2 + P_3 + R - (3P_1^\infty + R) = (l_1 \cdot C) - (3P_1^\infty + R) \sim (l_2 \cdot C) - (3P_1^\infty + R) = P_1^\infty + R + S + T - (3P_1^\infty + R) = S + T - 2P_1^\infty$.
Die Eindeutigkeit der Darstellungen (ii) und (iii) folgt sofort aus Lemma 3.1.1. □

Für hyperelliptische Kurven ist die Berechnung des Inversen einer Divisorenklasse trivial. Dies ist für nicht-hyperelliptische Kurven vom Geschlecht 3 nicht mehr der Fall: Möchte man z.B. das Inverse von $D = P_1 + P_2 + P_3 - (P_1^\infty + P_2^\infty + P_3^\infty)$ berechnen, so benötigt man dafür die Quadrik Q durch P_1, P_2, P_3 und $2P_4^\infty$. In diesem Fall gilt

$$D + (R_1 + R_2 + R_3 - (P_1^\infty + P_2^\infty + P_3^\infty)) \sim 0,$$

dabei sind R_1, R_2, R_3 die anderen Schnittpunkte von Q mit C.

Sei $D \in \mathrm{Div}_k^0(C)$ und D^+ ein effektiver Divisor mit $D^+ - D_3^\infty \sim D$. Im generischen Fall ist D^+ eindeutig bestimmt. „Par abus de language“ sagen wir eine Kurve C' *geht* durch nP, falls $i(C, C'; P) = n$, dabei ist $i(C, C'; P)$ die Schnittvielfachheit von C und C' an P.

Satz 3.2.2. Seien $D_1, D_2 \in \mathrm{Div}_k^0(C)$. Dann ist $D_1 + D_2$ äquivalent zum Divisor $D = D^+ - D_3^\infty$, wobei die Punkte auf dem Träger von D^+ durch den folgenden Algorithmus berechnet werden:

(i) Zuerst berechnet man die Kubik E, die durch den Träger von D_1^+, D_2^+ und $P_1^\infty, P_2^\infty, P_4^\infty$ geht (Multiplizität mitgezählt). Sei

$$D_3 := (C \cdot E) - (D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty).$$

(ii) Dann berechnet man die Quadrik Q, die durch den Träger von D_3 und P_1^∞, P_2^∞ geht. Es gilt: $D^+ := (C \cdot Q) - (D_3 + P_1^\infty + P_2^\infty)$.

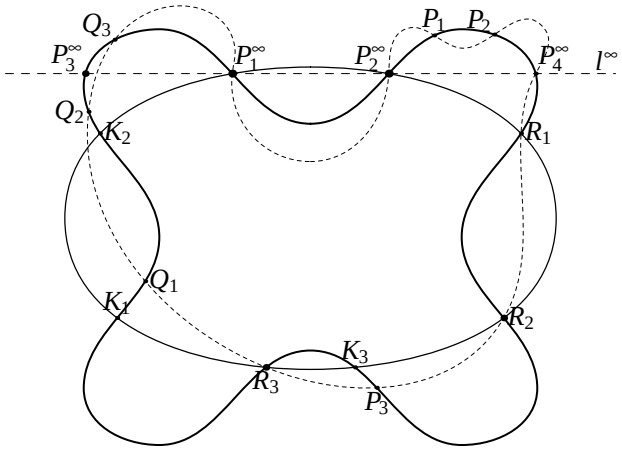


Abbildung 3.1: Beschreibung des Algorithmus von Satz 3.2.2

Bemerkung 3.2.2.

(i) Ist $P_1^\infty = P_2^\infty = P_4^\infty$, so gilt $D^+ - D_3^\infty \sim -(D_3 - D_3^\infty)$, denn

$$D^+ + D_3 + P_1^\infty + P_2^\infty \sim (C \cdot Q) \sim 2(C \cdot l_\infty) = 2D_3^\infty + 2P_4^\infty.$$

Mit anderen Worten: Die Kubik E liefert die Reduktion von $-(D_1 + D_2)$ und die Quadrik Q die Reduktion des Inversen von $-(D_1 + D_2)$.

(ii) Im generischen Fall ist die in Satz 3.2.2 erwähnte Kubik eindeutig bestimmt und irreduzibel. Falls es eine Quadrik Q_1 gibt, die durch den Träger von D_1^+ und D_2^+ geht, so kann $D_1 + D_2$ noch effizienter berechnet werden: nach dem Satz von Bézout trifft die Quadrik Q_1 die Kurve C in zwei weiteren Punkte K_1 und K_2:

$$D_1^+ + D_2^+ + K_1 + K_2 \sim 2K_C.$$

Sei dann l die Gerade durch K_1 und K_2, und seien R_1, R_2 die weiteren Schnittpunkte von l mit C. Dann gilt

$$K_1 + K_2 + R_1 + R_2 \sim K_C.$$

Es folgt

$$(D_1^+ - D_3^\infty) + (D_2^+ - D_3^\infty) \sim R_1 + R_2 + P_4^\infty - D_3^\infty.$$

Beweis von Satz 3.2.2. Wir können o.B.d.A. annehmen, dass C eine glatte ebene Quartik ist. In diesem Fall gilt $(E \cdot C) \sim 3K_C$, wobei K_C der kanonische Divisor

von C und $(E \cdot C)$ der Schnittdivisor von E mit C ist. Daraus ergibt sich

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_3 \sim 3K_C.$$

Analog folgt aus $(Q \cdot C) \sim 2K_C$, dass

$$D_3 + P_1^\infty + P_2^\infty + D_e \sim 2K_C,$$

für einen effektiven Divisor D_e vom Grad 3. Aus $(l^\infty \cdot C) = P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty \sim K_C$ und den zwei obigen Relationen folgt

$$D_1^+ + D_2^+ + P_1^\infty + P_2^\infty + P_4^\infty + D_3 \sim D_3 + P_1^\infty + P_2^\infty + D_e + P_1^\infty + P_2^\infty + P_3^\infty + P_4^\infty,$$

und somit

$$D_1^+ + D_2^+ \sim D_e + D_3^\infty.$$

Subtrahiert man $2D_3^\infty$ auf beiden Seiten der obigen Relation, so erhält man

$$D_1 + D_2 \sim D_e - D_3^\infty \sim D,$$

also $D_e = D^+$. □

3.2.2 Algebraische Durchführung des Algorithmus im generischen Fall

In diesem Abschnitt beschreiben wir eine algebraische Durchführung des Algorithmus in Satz 3.2.2. Genauer werden wir explizite Formeln für diesen Algorithmus entwickeln. Die Effizienz der algebraischen Version hängt von der Wahl von l^∞ ab. Der Algorithmus ist am effizientesten falls l^∞ eine Tangente an einen Hyperwendepunkt ist.

Zuerst möchten wir eine einfache Darstellung der Kurve (sowie ihrer reduzierten Divisoren) ableiten.

Sei im folgenden C eine glatte ebene Quartik, so dass $(*)$ erfüllt ist. Nach Anwendung einer k-linearen Transformation können wir annehmen, dass l^∞ die Gerade mit der Gleichung $z = 0$ und $P_1^\infty = (0 : 1 : 0)$. Sei $F(x, y) = 0$ ein affine Gleichung für C. Wie bei hyperelliptischen Kurven führen wir die *Mumford-Darstellung* $(u, v) \in k[x]^2$ von reduzierten Divisoren $D \in \mathrm{Div}_k^0(C)$ ein. Diese ist im generischen Fall (**typischer Divisor**) eindeutig bestimmt:

(i) Die Elemente des Trägers von D^+ sind nicht kollinear.

(ii) Auf dem Träger von D^+ liegen keine *unendlich fernen* Punkte P_i^∞. Seien $P_i = (x_i : y_i : 1)$ $(i = 1, 2, 3)$ die drei Punkte auf dem Träger von D^+ und $u = \prod(x - x_i)$. Da D^+ ein k-rationaler Divisor ist, liegt u in $k[x]$.

(iii) Die $(x_i)_{i=1,2,3}$ sind paarweise verschieden. In diesem Fall, existiert ein eindeutiges Polynom $v \in k[x]$ vom Grad 2, so dass $y_i = v(x_i)$ ist für $i = 1, 2, 3$ (v ist das Interpolationspolynom durch die P_i).

Für ein Paar $(u, v) \in k[x]^2$ mit

- $u, v \in k[x]$,
- $u = \prod(x - x_i)$ ein normiertes Polynome vom Grad 3 mit nur einfachen Nullstellen,
- $\deg(v) = 2$,
- $u | F(x, v(x))$,

ist umgekehrt der Divisor $P_1 + P_2 + P_3 - D_3^\infty$ mit $P_i = (x_i : v(x_i) : 1)$ ein k-rationaler typischer Divisor von C.

Die Summe zweier typischer Divisoren ist im generischen Fall ein typischer Divisor.

Wir werden im folgenden nur den Algorithmus für typische Divisoren erläutern, da dies für unsere kryptographische Anwendungen ausreicht. Der vollständige Algorithmus (für alle Fälle) wurde ebenfalls implementiert und ist unter

`http://www.exp-math.uni-essen.de/~oyono`

aufrufbar.

l^∞ ist eine Tangente

Nach einer k-linearen Transformation können wir annehmen, dass l^∞ eine Tangente an $P_1^\infty = (0 : 1 : 0)$ ist. Weiterhin können wir annehmen, dass l^∞ durch $P_4^\infty = (1 : 0 : 0)$ geht. Dann besitzt C eine Gleichung der Gestalt

$$y^3 + h_1(x)y^2 + h_2(x)y = f(x),$$

mit $h_1(x), h_2(x), f(x) \in k[x]$ und $\deg h_1(x) \leq 2, \deg h_2(x) \leq 3, \deg f(x) \leq 3$.

Lemma 3.2.1. Die Kubik E von Satz 3.2.2 ist im generischen Fall von der Form

$$y^2 + s(x) \cdot y + t(x),$$

wobei $s(x)$ und $t(x)$ Polynome mit $\deg s(x) \leq 2$ und $\deg t(x) \leq 2$ sind.
Die Quadrik Q ist von der Form

$$y - v(x),$$

mit $v(x) \in k[x]$ und $\deg v(x) = 2$.

Beweis.

(i) Sei $t_{P_1^\infty} : z = 0$ die Tangente an C durch P_1^∞. Sei

$$E = a_{00}y^3 + y^2(a_{10}x + a_{01}z) + y(a_{20}x^2 + a_{11}xz + a_{02}z^2) + (a_{30}x^3 + a_{21}x^2z + a_{12}xz^2 + a_{03}z^3).$$

Die Kubik E geht genau dann durch P_1^∞ wenn $a_{00} = 0$. Die Tangente an E durch P_1^∞ besitzt die Gleichung

$$\left(\frac{\partial E}{\partial x}(0:1:0)\right) x + \left(\frac{\partial E}{\partial y}(0:1:0)\right) y + \left(\frac{\partial E}{\partial x}(0:1:0)\right) z = a_{10}x + a_{01}z.$$

Die Kubik E geht somit genau dann durch $2P_1^\infty$ wenn $a_{01} \neq 0$ und $a_{10} = a_{00} = 0$. Ferner geht E durch $(1:0:0)$ genau dann wenn $a_{30} = 0$.

(ii) Der Beweis ist analog zu (i).

□

Der Algorithmus in Satz 3.2.2 kann in 3 Schritten unterteilt werden:

(i) Berechne die Kubik E,

(ii) berechne die Quadrik Q,

(iii) berechne die reduzierte Darstellung von $D_1 + D_2$.

Schritt 1: Berechnung der Kubik E

Nur in diesem Schritt werden wir zwischen Addition und Verdopplung unterscheiden.

Addition

Wir betrachten nun den generischen Fall, d.h. die Kubik E ist gegeben durch die Gleichung

$$E : h(x, y) = y^2 + s(x) \cdot y + t(x) = 0$$

mit Polynomen $s(x)$ und $t(x)$ mit $\deg s(x) \leq 2$ und $\deg t(x) \leq 2$. Division mit Rest von $y^2 + sy + t$ durch $y - v_i$ liefert $y^2 + sy + t = (y - v_i)(y + v_i + s) + r_i$ mit $r_i(x) \in k[x]$ vom Grad $\deg r_i(x) \leq 4$. Da der Träger von D_1 (bzw. D_2) im Träger von $(C \cdot E)$ enthalten ist, folgt $r_i(x) = u_i(x) \cdot \delta_i(x)$ mit $\deg \delta_i(x) = 1$. Daher reduziert sich die Suche von E auf das Auffinden dreier Polynome $s(x), \delta_1(x)$ und $\delta_2(x)$ in $k[x]$ mit $\deg s(x) = 2$, $\deg \delta_1(x) = \deg \delta_2(x) = 1$, so dass

$$h(x, y) = (y - v_1) \cdot (y + v_1 + s) + u_1 \cdot \delta_1 = (y - v_2) \cdot (y + v_2 + s) + u_2 \cdot \delta_2. \quad (3.1)$$

Dies führt auf die Gleichung

$$(v_1 + v_2 + s) \cdot (v_1 - v_2) + u_2 \cdot \delta_2 - u_1 \cdot \delta_1 = 0. \quad (3.2)$$

Im nicht-generischen Fall besitzt E keinen y^2 Term, und eine analoge Strategie führt auf die Gleichung

$$s \cdot (v_1 - v_2) + \delta_2 \cdot u_2 - \delta_1 \cdot u_1 = 0, \quad (3.3)$$

wobei $\delta_1(x)$ und $\delta_2(x)$ konstante Polynome sind.

Man beachte, dass die beiden Gleichungen (3.2) und (3.3) ähnlich sind: während der Bestimmung von $s(x)$ und $\delta_1(x)$ berechnen wir nämlich in beiden Fällen den Rest $r(x)$ der euklidischen Division von $t_1(x) \cdot (u_1(x) - u_2(x))$ durch $u_2(x)$, wobei $t_1(x)$ das Inverse von $(v_1(x) - v_2(x))$ modulo $u_2(x)$ ist. Durch einfache Berechnungen sieht man, dass $r(x)$ genau dann vom Grad 2 ist, wenn wir im Fall (3.2) sind.

Verdopplung

In diesem Fall ist E ein Element des Ideals $I^2 = \langle u_1^2, u_1(y - v_1), (y - v_1)^2 \rangle$. Wie im Fall der Addition betrachten wir nur den generischen Fall, in dem sich E in der Form

$$(y - v_1) \cdot (y + v_1 + s) + u_1\delta_1 \quad (3.4)$$

schreiben lässt.

Die anderen Fällen sind entweder trivial oder leichter zu beschreiben und treten sehr selten auf. Wie oben genügt E der folgenden Relation

$$(y - v_1)(2v_1 + s) + u_1\delta_1 \in I^2. \quad (3.5)$$

Andererseits gilt

$$\left(3v_1^2 + 2v_1h_1 + h_2\right)(y - v_1) + u_1w_1 \in I^2, \quad (3.6)$$

wobei $w_1(x) \in k[x]$ mit

$$\begin{aligned} u_1 \cdot w_1 &= v_1^3 + v_1^2 h_1 + v_1 h_2 - f \\ &= v_1^3 + v_1^2 h_1 + v_1 h_2 - (y^3 + h_1 y^2 + h_2 y) \\ &= (v_1 - y)^3 - (v_1 - y)^2 \cdot (3v_1 + h_1) + (v_1 - y) \cdot (3v_1^2 + 2v_1 h_1 + h_2). \end{aligned}$$

Daraus folgt nun

$$\left(3v_1^2 + 2v_1 h_1 + h_2\right) u_1 \delta_1 + (2v_1 + s) u_1 w_1 \in I^2,$$

und somit

$$-\left(3v_1^2 + 2v_1 h_1 + h_2\right) \delta_1 + (2v_1 + s) w_1 \equiv 0 \mod u_1. \tag{3.7}$$

Die Berechnung des Inversen von $w_1(x)$ in $k[x]/(u_1(x))$ liefert unmittelbar $\delta_1(x)$ und $s(x)$.

Bemerkung 3.2.3. Sind $3v_1^2 + 2v_1 h_1 + h_2$ und u_1 teilerfremd, so sind (3.5) und (3.7) äquivalent.

Schritt 2: Berechnung der Quadrik Q

Wir betrachten nur den generischen (und schwierigsten) Fall. Die in Schritt 1 berechnete Kubik ist von der Form

$$E : h(x, y) = y^2 + s(x) \cdot y + t(x)$$

mit $s(x), t(x) \in k[x]$, $\deg s(x) \leq 2$ und $\deg t(x) \leq 2$.

Um die Quadrik Q zu bestimmen, berechnet man erst die y-Resultante $\mathrm{Res}_y(E, C)$ von E und $y^3 + h_1(x)y^2 + h_2(x)y - f(x)$

$$\begin{aligned} \mathrm{Res}_y(E, C) &= t^3 + f s^3 - 3fts + f^2 \\ &\quad + h_2\left(t(s^2 - t - s h_1 + h_2 - t) + fs\right) \\ &\quad + h_1\left(t(f - st + h_1 t) - f(s^2 - t)\right) \end{aligned} \tag{3.8}$$

und dann den normierten Quotienten $\tilde{u}$ der Division von $\mathrm{Res}_y(E, C)$ durch $u_1 u_2$.

Aus $E \in \langle y - v, \tilde{u} \rangle$ und aus

$$\begin{aligned} -\left(yE - (y^3 + h_1 y^2 + h_2 y - f) - (s - h_1)E\right) = \\ \left(-t + s^2 + h_2 - s h_1\right) y + \left(-f + ts - t h_1\right), \end{aligned} \tag{3.9}$$

folgt für die Quadrik $Q = y - v(x)$

$$\left(t - h_2 + sh_1 - s^2\right) v \equiv (st - th_1 - f) \mod \tilde{u}. \tag{3.10}$$

Das Polynom $v(x)$ ist somit der Rest der euklidischen Division von

$$\alpha_1 \left(st - th_1 - f\right)$$

durch $\tilde{u}(x)$, wobei $\alpha_1(x)$ das Inverse von

$$t(x) - h_2(x) + s(x)h_1(x) - s^2(x)$$

in $k\left[x, y\right] / (\tilde{u}(x))$ ist.

Schritt 3: Berechnung von $D_1 + D_2$

Schließlich gilt

$$v_{D_1+D_2}(x) = v(x).$$

Ist $v_{D_1+D_2}(x)$ bekannt, so ist das normierte Polynom $u_{D_1+D_2}(x)$ leicht zu berechnen, nämlich als normierter Quotient von

$$v_{D_1+D_2}^3 + v_{D_1+D_2}^2 h_1 + v_{D_1+D_2} h_2 - f \tag{3.11}$$

durch $\tilde{u}(x)$.

Algorithmus 3 Addition in der Jacobischen glatter Quartiken.

INPUT: $D_1 = (u_1, v_1)$ und $D_2 = (u_2, v_2)$
OUTPUT: $D_1 + D_2 = (u_{D_1+D_2}, v_{D_1+D_2})$

1. *Berechnung der Kubik E*

Addition

Berechne das Inverse t_1 von $v_1 - v_2$ modulo u_2.
Berechne den Rest r der Division von $(u_1 - u_2)t_1$ durch u_2.
Löse das lineare Gleichungssystem gegeben durch

$$\begin{cases} \deg_x(-v_1(v_1+s)+u_1\delta_1) = 2 & (2\text{ Gl.}) \\ v_1 + v_2 + s \equiv r\delta_1 \mod u_2 & (3\text{ Gl.}) \end{cases}$$

wobei $s, \delta_1 \in k[x]$ mit $\deg(s) = 2$ und $\deg(\delta_1) = 1$. Setze

$$E = (y - v_1)(y + v_1 + s) + u_1\delta_1.$$

Verdopplung

Berechne $\omega_1 = (v_1^3 + v_1^2 h_1 + v_1 h_2 - f)/u_1$.
Berechne das Inverse t_1 von ω_1 modulo u_1.
Berechne den Rest r von $(3v_1^2 + 2v_1h_1 + h_2)t_1$ durch u_1.
Löse das lineare Gleichungssystem gegeben durch

$$\begin{cases} \deg_x(-v_1(v_1+s)+u_1\delta_1) = 2 & (2\text{ Gl.}) \\ 2v_1 + s \equiv r\delta_1 \mod u_1 & (3\text{ Gl.}) \end{cases}$$

wobei $s, \delta_1 \in k[x]$ mit $\deg(s) = 2$ und $\deg(\delta_1) = 1$. Setze

$$E = (y - v_1)(y + v_1 + s) + u_1\delta_1.$$

2. *Berechnung der Quadrik Q*

Berechne $\tilde{u} := Res_y^*(E, C)/(u_1u_2)$.
Berechne das Inverse α_1 von $t - s^2 - h_2 + sh_1$ modulo $\tilde{u}$.
Berechne den Rest v von $\alpha_1(st - th_1 - f)$ durch $\tilde{u}$. Setze

$$Q = y - v.$$

3. *Berechnung von* $D_1 + D_2$

$v_{D_1+D_2} := v$
$u_{D_1+D_2} := ((v^3 + v^2h_1 + vh_2 - f)/(\tilde{u}))^*$
$D_1 + D_2 = (u_{D_1+D_2}, v_{D_1+D_2})$

Bezeichnung 3.2.1. Für $g \in k[x]$ bezeichnen wir mit g^* den Quotienten von g durch seinen Leitkoeffizienten.

Bemerkung 3.2.4.

(i) Die Wahl von $D^\infty = D_3^\infty$ war so bestimmt, dass die Quadrik Q von der einfachen Form $y - v(x)$ ist. Dies liefert somit den zweiten Teil der Mumford-Darstellung von $D_1 + D_2$. Andere Wahlen von D^∞ können dazu führen, dass man eine zusätzliche Quadrik für die Bestimmung von $v_{D_1+D_2}(x)$ berechnen muss.

(ii) Der Algorithmus 3 kann auf jeden Körper angewendet werden (also auch auf Körper k mit $\mathrm{char}(k) = 0$).

l^∞ ist Tangente an einem Weierstrass-Punkt

Sei $k = \mathbb{F}_q$ ein Körper mit $\mathrm{char}(k) > 3$. Sei $C : F = 0$ eine glatte Quartik und $H : h = 0$ ihre Hessesche. Die Wendepunkte von C entsprechen genau den 24 Schnittpunkten von C mit H (mit Multiplizität gezählt). Im generischen Fall können wir für $q \gg 0$ annehmen, dass zwei Wendepunkte von C verschiedene Koordinaten haben. Unter dieser Annahme besitzt C mindestens einen k-rationalen Wendepunkt, genau dann wenn das Polynom $\mathrm{Res}_y(F, h)$ eine Nullstelle in k besitzt. Sei $(\alpha_i)_{i\in\{1,\cdots,q\}}$ eine Anordnung von $\mathbb{F}_q$.
Sei S die Menge der normierten Polynome vom Grad n in $k[x]$ und S_i die Untermenge von S bestehend aus Polynomen, die mindestens einen Faktor der Form $x - \alpha_i$ $(i = 1, \cdots, q)$ besitzen. Dann ist $|S| = q^n$ und $|S_i| = q^{n-1}$. Nach dem *Inklusions-Exklusions* Prinzip ist die Anzahl $N(n, q)$ der normierten Polynome vom Grad n, die mindestens einen Linearfaktor haben, gegeben durch

$$N(n,q) = \sum_{i=1}^{n} \binom{q}{i} q^{n-i}(-1)^{i-1} \quad \text{mit} \quad \binom{q}{i} = 0 \text{ für } \; i \geq q.$$

Lemma 3.2.2. Die Wahrscheinlichkeit $P(n, q)$, dass ein normiertes Polynom vom Grad n mindestens einen Linearfaktor in $\mathbb{F}_q[x]$ besitzt, ist gegeben durch

$$P(n,q) = 1 - \left(1 - \frac{1}{q}\right)^q - \alpha(n,q),$$

wobei $\alpha(n, q) = 0$ für $n \geq q$ und

$$\left|\alpha(n,q)\right| \leq \frac{1}{(n+1)!}$$

für $n < q$. Ferner gilt

$$\lim_{\substack{n<q \\ n,q\to\infty}} \alpha(n,q) = 0.$$

Beweis. Wegen $(q-1)^q = \sum_{k=0}^{q} \binom{q}{k} q^{q-k}(-1)^k$ folgt für $n \geq q$

$$N(n,q) = q^n - (q-1)^q q^{n-q},$$

und für $n < q$

$$N(n,q) = q^n - (q-1)^q q^{n-q} - \left(\sum_{k=n+1}^{q} q^{q-k} \binom{q}{k} (-1)^k \right) q^{n-q},$$

und somit

$$P(n,q) = \frac{N(n,q)}{q^n} = 1 - \left(1 - \frac{1}{q}\right)^q - \alpha(n,q),$$

mit $\alpha(n,q) = 0$ für $n \geq q$ bzw. $\alpha(n,q) = \sum_{k=n+1}^{q} a_k(-1)^k$ mit $a_k := \binom{q}{k} q^{-k}$ für $n < q$. Für die streng monoton fallende Folge (a_k) gilt $0 < a_k < \frac{1}{k!}$, und deshalb für die alternierende Summe $\alpha(n,q)$ gilt:

$$\left|\alpha(n,q)\right| \leq \frac{1}{(n+1)!}.$$

□

Wir erhalten folgende Vermutung, falls wir zusätzlich annehmen, dass $(F,h) \mapsto \mathrm{Res}_y(F,h)$ über der Menge der Polynome in $\mathbb{F}_q[x]$ vom Grad 24 gleichmäßig verteilt ist.

Vermutung 3.2.1. Die Wahrscheinlichkeit, dass eine glatte ebene Quartik mindestens einen rationalen Wendepunkt besitzt, ist asymptotisch gleich

$$1 - e^{-1} + \alpha, \text{ mit } |\alpha| \leq 10^{-25},$$

für $q \longrightarrow \infty$.

Bemerkung 3.2.5. Wir haben die obige Vermutung auf Richtigkeit getestet: Die Untersuchung von 10^6 glatten ebenen Quartiken über $\mathbb{F}_{1009^2}$ (bzw. $\mathbb{F}_{2^{17}+29}$) liefern die erwarteten Verhältnisse. Auch im Falle von Körpern der Charakteristik 2 und 3 erhalten wir dieselbe Heuristik.

p	**n**	**Wahrscheinlichkeiten**
2	17	$632074/10^6 = 0.632074$
3	11	$632344/10^6 = 0.632344$
1009	2	$631358/10^6 = 0.631358$
$2^{17} + 29$	1	$632921/10^6 = 0.632921$

Gibt es einen Wendepunkt in $C(k)$, so können wir nach einer k-linearen Transformation annehmen, dass $l = l^\infty$ die Tangente an den Wendepunkt $P_1^\infty = (0 : 1 : 0)$ ist. In diesem Fall besitzt die Kurve C ein affines Modell der Form

$$y^3 + h_1(x)y^2 + h_2(x)y = f(x),$$

mit $h_1(x), h_2(x), f(x) \in k[x]$ und $\deg h_1(x) \leq 1, \deg h_2(x) \leq 3, \deg f(x) \leq 4$.

Ebenso erhalten wir wie in Lemma 3.2.1:

Lemma 3.2.3. Die Kubik E ist im generischen Fall von der Form

$$y^2 + s(x) \cdot y + t(x),$$

wobei $s(x)$ und $t(x)$ Polynome in x mit $\deg s(x) \leq 1$ und $\deg t(x) \leq 3$ sind.
Die Quadrik Q ist von der Form

$$y - v(x),$$

mit $v(x) \in k[x]$ und $\deg v(x) = 2$.

Beweis.

(i) Sei $t_{P_1^\infty} : z = 0$ die Tangente an C durch P_1^∞. Sei

$$E = a_{00}y^3 + y^2(a_{10}x + a_{01}z) + y(a_{20}x^2 + a_{11}xz + a_{02}z^2) + (a_{30}x^3 + a_{21}x^2z + a_{12}xz^2 + a_{03}z^3).$$

Die Kubik E geht genau dann durch P_1^∞ wenn $a_{00} = 0$. Die Tangente an E durch P_1^∞ besitzt die Gleichung

$$\left(\frac{\partial E}{\partial x}(0:1:0)\right)x + \left(\frac{\partial E}{\partial y}(0:1:0)\right)y + \left(\frac{\partial E}{\partial x}(0:1:0)\right)z = a_{10}x + a_{01}z.$$

Die Kubik E geht somit durch $2P_1^\infty$ genau dann wenn $a_{01} \neq 0$ und $a_{10} = a_{00} = 0$. Ferner geht E durch $3P_1^\infty$ genau dann wenn $E \cap t_{P_1^\infty} = \{P_1^\infty\}$, also wenn die Gleichung

$$0 = a_{30}x^3 + a_{20}x^2y = x^2(a_{30}x + a_{20}y)$$

nur die Lösung $x = 0$ besitzt, m.a.W. ist $a_{20} = 0$.

(ii) Der Beweis ist analog zu (i).

□

Der einzige Unterschied zum Algorithmus 3 ist, dass $s(x)$ und $\delta_1(x)$ nun Polynome vom Grad 1 sind. Deswegen sind hier die Berechnungen von E und Q viel einfacher: das lineare Gleichungssystem in Schritt 1

$$\begin{cases} \deg_x(-v_1(v_1+s)+u_1\delta_1) = 3 \\ v_1+v_2+s \equiv r\delta_1 \qquad \bmod u_2 \end{cases}$$

besteht nun aus vier statt fünf Gleichungen, und folglich ist auch die Resultante $\mathrm{res}_y(E,C)$ leichter zu berechnen.
Falls ferner $\mathrm{char}(k) \neq 3$ ist, so können wir zusätzlich mittels Tschirnhaus-Transformationen annehmen, dass C ein Modell der folgenden Form besitzt

$$y^3 + h_2(x)y = f(x),$$

mit $h_2(x)$ und $f(x)$ wie oben. Auch können wir im Falle $\mathrm{char}(k) \neq 2$ weiterhin annehmen, dass der x^3-Koeffizient von $f(x)$ verschwindet.
Mit dieser Darstellung von $f(x)$ sind (für Addition und Verdopplung) Schritte 2 und 3 schneller. Außerdem ist Schritt 1 etwas schneller für die Verdopplung. In diesem Fall kostet eine Addition $148M + 15SQ + 2I$ und eine Verdopplung $165M + 20SQ + 2I$. Eine detaillierte Beschreibung zur Entwicklung der expliziten Formeln befindet sich in Abschnitt 3.2.3.

l^∞ ist Tangente an einem Hyperwendepunkt

Sei C eine glatte ebene Quartik, die einen Hyperwendepunkt P^∞ besitzt. Durch k-lineare Transformationen können wir erreichen, dass $P^\infty = (0:1:0)$ ist, und dass die Tangente an P^∞ die Gerade mit der Gleichung $z = 0$ ist. Die Quartik C besitzt dann ein Modell mit der Gleichung

$$y^3 + h_1(x)y^2 + h_2(x)y = f(x),$$

wobei $h_i(x)$ ein Polynom vom Grad i und $f(x)$ ein Polynom vom Grad 4 ist. Insbesondere ist C eine C_{34}-Kurve.
Falls $\mathrm{char}(k) \neq 3$ ist, können wir weiterhin $h_1(x) = 0$ annehmen. Gilt zusätzlich $\mathrm{char}(k) \neq 2$, so verschwindet der x^3-Koeffizient von $f(x)$.

Eine Addition kostet $131M + 14SQ + 2I$ und eine Verdopplung $148M + 19SQ + 2I$ (siehe Abschnitt 3.2.3).

Bemerkung 3.2.6. Besitzt C einen Hyperwendepunkt P^∞, so sind $\mathrm{Jac}(C)(k)$ und die Idealklassengruppe von $k[x,y]/(F(x,y))$ isomorph.

C ist eine Picard-Kurve

Sei C eine Picard-Kurve mit dem affinen Modell

$$y^3 = f(x),$$

wobei $f(x)$ ein normiertes Polynom vom Grad 4 ist, das nur einfache Nullstellen in $\bar{k}$ besitzt. Ist $\mathrm{char}(k) \neq 3$, so sind Picard-Kurven zyklische trigonale Kurven vom Geschlecht 3 mit einer zyklischen Galois-Überlagerung $\pi : C \xrightarrow{3:1} \mathbb{P}^1(\bar{k})$, die genau fünf Verzweigungspunkte besitzt. Diese sind total verzweigt. Die Automorphismengruppe der Überlagerung π ist durch

$$\sigma : (x : y : z) \longmapsto (x : \zeta_3 y : z)$$

erzeugt. Dabei ist ζ_3 eine nicht-triviale dritte Einheitswurzel.

Für $q \equiv 2 \pmod 3$ liefern Picard-Kurven kryptographisch ungeeignete Kurven:

Lemma 3.2.4. Sei C eine Picard-Kurve über $\mathbb{F}_q$ mit $q \equiv 2 \mod 3$. Dann zerfällt das L-Polynom von C über $\mathbb{Q}$. Genauer gilt: die Ordnung der Jacobischen ist durch $q+1$ teilbar.

Beweis. Sei $N_r := \#C(\mathbb{F}_{q^r}) - (q^r + 1)$ für $r = 1, 2, 3$. Das L-Polynom von C ist dann gleich

$$L(t) = \sum_{i=0}^{6} c_i t^i$$

mit $c_{6-i} = q^{3-i} c_i$ für $i = 0, 1, 2$ und

$$c_1 = N_1, \quad c_2 = \frac{1}{2}\left(N_2 + N_1^2\right), \quad c_3 = \frac{1}{3}\left(N_3 + \frac{3}{2}N_1 N_2 + \frac{1}{2}N_1^3\right). \tag{3.12}$$

Ist $q \equiv 2 \mod 3$, so besitzt die Gleichung $y^3 = a$ für jedes $a \in \mathbb{F}_q$ genau eine Lösung in $\mathbb{F}_q$, woraus $N_1 = N_3 = 0$ folgt. Aus (3.12) ist N_2 gerade und somit folgt

$$L(t) = (qt^2 + 1)(q^2 t^4 + \frac{N_2}{2} t^2 - qt^2 + 1),$$

also: $(q+1) | L(1) = \#\mathrm{Jac}(C)(\mathbb{F}_q)$. □

Der Algorithmus 3 ist wegen der niedrigen Anzahl der Koeffizienten von C noch effizienter als mit gewöhnlichen C_{34}-Kurven. Eine Addition kostet hier $116M + 14SQ + 2I$ und eine Verdopplung $133M + 19SQ + 2I$ (siehe Abschnitt 3.2.3).

Ein weiterer Vorteil für die Verwendung Picard-Kurven in der Kryptographie besteht aus der Möglichkeit, die Skalarmultiplikation effizient zu berechnen: Die Kosten der Berechnung der Skalarmultiplikation können halbiert werden, indem man die -2-adische Methode (siehe Abschnitt 3.2.5) und die GLV-Methode basierend auf dem schnellen Automorphismus σ – wie in [27] für spezielle elliptische Kurven vorgestellt – verwendet.

3.2.3 Explizite Formeln

Arithmetik in $k[x]$

In diesem Abschnitt werden wir Methoden zur Beschleunigung der Arithmetik in $k[x]$ beschreiben.

Sei $M(m, n)$ die Anzahl der Multiplikationen (im Grundkörper k), für die die Multiplikation zweier Polynome f und g vom Grad $n-1$ und $m-1$ notwendig ist. Mit der naiven *Schoolbook* Multiplikation benötigt man $m \cdot n$ Multiplikationen.

Karatsuba-Ofman Multiplikation

Um die Anzahl der Multiplikationen im Grundkörper zu reduzieren, haben Karatsuba-Ofman folgende Trick angewendet

$$(ax + b)(cx + d) = acx^2 + x\left((a + b)(c + d) - (ac + bd)\right) + bd,$$

was eine Verbesserung im Vergleich zur naiven *Schoolbook* Methode liefert.

Diese Vorgehensweise [49] kann natürlich auf Polynome beliebigen Grades erweitert werden: Sind z.B. f und g Polynome vom Grad $2n-1$ mit

$$\begin{aligned} f(x) &= \sum_{i=0}^{2n-1} f_i x^i = \sum_{i=0}^{n-1} f_i x^i + x^n \sum_{i=0}^{n-1} f_{i+n} x^i =: a(x) + x^n b(x) \\ g(x) &= \sum_{i=0}^{2n-1} g_i x^i = \sum_{i=0}^{n-1} g_i x^i + x^n \sum_{i=0}^{n-1} g_{i+n} x^i =: c(x) + x^n d(x) \end{aligned}$$

so gilt

$$f(x)g(x) = u(x) + x^n\left(w(x) - (u(x) + v(x))\right) + x^{2n} v(x),$$

wobei

$$\begin{aligned} u(x) &= a(x)c(x), \\ v(x) &= b(x)d(x), \\ w(x) &= (a(x)+b(x))(c(x)+d(x)). \end{aligned}$$

Toom-Cook Multiplikation

Der **Toom-Cook** Algorithmus [12] basiert auf Bewertungen und Interpolation: Um das Produkt $h(x) := f(x) \cdot g(x)$ zweier Polynome f und g vom Grad $n-1$ zu bestimmen, berechnet man erst $f(\alpha_i)$ und $g(\alpha_i)$ an $2n-1$ verschiedenen Stellen. Dann ermittelt man mit Hilfe der $2n-1$ Produkte $h(\alpha_i) = f(\alpha_i) \cdot g(\alpha_i)$ mittels Lagrange Interpolation das Polynom $h(x)$

$$h(x) = \sum_{j=0}^{2n-2} h(\alpha_j) \prod_{k \neq j} \frac{x - x_k}{\alpha_j - \alpha_k}$$

durch die $2n-1$ Punkten $(\alpha_i, h(\alpha_i))$.

Sind die α_i klein, so treten bei der Berechnung von $h(x)$ nur Divisionen mit kleinen Zahlen auf.

Beispiel 3.2.1. Seien $f(x) = f_2x^2 + f_1x + f_0,\ \ g(x) = g_2x^2 + g_1x + g_0$ und

$$h(x) = f(x) \cdot g(x) =: h_4x^4 + h_3x^3 + h_2x^2 + h_1x + h_0.$$

Dann gilt

$$\begin{aligned} h(0) &= h_0 = f_0 \cdot g_0 \\ h(1) &= h_0 + h_1 + h_2 + h_3 + h_4 = (f_0 + f_1 + f_2) \cdot (g_0 + g_1 + g_2) \\ h(2) &= h_0 + 2h_1 + 4h_2 + 8h_3 + 16h_4 = (f_0 + 2f_1 + 4f_2) \cdot (g_0 + 2g_1 + 4g_2) \\ h(-1) &= h_0 - h_1 + h_2 - h_3 + h_4 = (f_0 - f_1 + f_2) \cdot (g_0 - g_1 + g_2) \\ h(-2) &= h_0 - 2h_1 + 4h_2 - 8h_3 + 16h_4 = (f_0 - 2f_1 + 4f_2) \cdot (g_0 - 2g_1 + 4g_2) \end{aligned}$$

und somit auch

$$\begin{aligned}
h_0 &= h(0)\\
h_1 &= \frac{2}{3}h(1) - \frac{1}{12}h(2) - \frac{2}{3}h(-1) + \frac{1}{12}h(-2)\\
h_2 &= -\frac{5}{4}h(0) + \frac{2}{3}h(1) - \frac{1}{24}h(2) + \frac{2}{3}h(-1) - \frac{1}{24}h(-2)\\
h_3 &= -\frac{1}{6}h(1) + \frac{1}{12}h(2) + \frac{1}{6}h(-1) - \frac{1}{12}h(-2)\\
h_4 &= \frac{1}{4}h(0) - \frac{1}{6}h(1) + \frac{1}{24}h(2) - \frac{1}{6}h(-1) + \frac{1}{24}h(-2).
\end{aligned}$$

Die folgende Tabelle liefert einen Vergleich für die Multiplikation von Polynomen kleinen Grades: Multiplikationen bzw. Divisionen mit kleinen ganzen Zahlen (hier $2, 3$ und 5) werden nicht gezählt.

Methoden	$M(2,2)$	$M(2,3)$	$M(2,4)$	$M(3,3)$	$M(3,4)$	$M(4,4)$
naiv	4	6	8	9	12	16
Karatsuba	3	5	6	6	8	9
Toom-Cook	3	4	5	5	6	7

Erweiterter Euklidischer Algorithmus

Für die Berechnung des $\mathrm{ggt}(f, g)$ zweier Polynome benutzen wir den in [6] beschriebenen erweiterten Euklidischen Algorithmus. Mit der Eingabe $f, g \in k[x]$ berechnet er die Polynome a, b und $d = \mathrm{ggt}(f, g)$ in $k[x]$ mit $af + bg = d$. Die Kosten der für uns interessanten Berechnungen fassen wir in der folgenden Tabelle zusammen:

f normiert, $\deg f = 3, \deg g = 2$	g normiert, $\deg g = 3, \deg f = 3$	g normiert, $\deg g = 3, \deg f = 4$
$13M + 2SQ$ für d und a	$16M + 2SQ$ für d und b	$17M + 2SQ$ für d und b

Auch werden wir den Rest der Division zweier Polynome berechnen. Sei $f = q \cdot g + r$ mit $\deg r < \deg g$: Ist g normiert und $\deg g = 3$ und $\deg f = 4$, so kostet die Berechnung von r genau $4M$. Sind aber f und g normiert mit $\deg f = 6, \deg g = 3$, so kostet die Berechnung von r genau $3M$.

Detaillierte Beschreibung der expiziten Formeln

In diesem Abschnitt erläutern wir Schritt für Schritt unsere Optimierungen zur Verbesserung der Komplexität der Gruppenoperation auf der Jacobischen nicht-hyperelliptischer Kurven vom Geschlecht 3.

Um den Algorithmus noch effizienter zu machen, verwenden wir folgenden Optimierungen:

(i) In Abhängigkeit der verwendeten Bibliothek für die Arithmetik in endlichen Körpern kostet eine Inversion zwischen 3 und 20 Multiplikationen. Um die Anzahl der Inversionen im Grundkörper zu reduzieren verwenden wir den Trick von Montgomery: statt die n Inversionen $a_1^{-1}, \ldots, a_n^{-1}$ einzeln durchzuführen, berechnen wir die *simultane* Inversion $(a_1 \cdot \cdots \cdot a_n)^{-1}$ und dann die Produkte

$$a_i^{-1} = (a_1^{-1} \cdot \cdots \cdot a_n)^{-1} \cdot a_1 \cdot \cdots \cdot a_{i-1} \cdot a_{i+1} \cdot \cdots \cdot a_n.$$

(ii) Um Polynome miteinander zu multiplizieren verwenden wir die Methoden von Karatsuba-Ofman und Toom-Cook (falls $p \neq 2, 3, 5$), und berechnen nur die Koeffizienten, die wir später verwenden werden. Als Beispiel: da die Resultante von E und C im Algorithmus 3 nur bei der Berechnung vom Quotienten der Division von $\mathrm{Res}_y(E, C)$ durch $u_1(x)u_2(x)$ auftritt, ist nur der Teil der Resultante mit Monomen x^i mit $i \geq 6$ relevant.

Wir betrachten hier nur die Addition zweier typischer Divisoren $D_1 = (u_1, v_1)$ und $D_2 = (u_2, v_2)$ mit $u_i = x^3 + u_{i2}x^2 + u_{i1}x + u_{i0}, v_i = v_{i2}x^2 + v_{i1}x + v_{i0}$.

Weiterhin betrachten wir nur den Fall, dass die Kurve C einen k-rationalen Wendepunkt besitzt, so dass C ein affines Modell der Form

$$C: \; y^3 + h(x)y - f(x) = 0$$

mit $h(x) := h_3x^3 + h_2x^2 + h_1x + h_0, \; f(x) := x^4 + f_2x^2 + f_1x + f_0$ in $k[x]$ hat. Mit E_y bzw. E_x bezeichnen wir die bezüglich y^2 bzw. x^3 normierte Darstellung der Kubik E.

Berechnung der Kubik E_y ***und der Resultante*** $Res_y(E_y, C)$

Für die in Algorithmus 3 definierte normierte Kubik E_y

$$E_y = y^2 + s_y y + t_y,$$

gibt es Elemente $\gamma_1, \gamma_2 \in k$, so dass

$$E_y = (y - v_1)(y + v_1 + s_y) + u_1(v_{12}^2 x + \gamma_1) = (y - v_2)(y + v_2 + s_y) + u_2(v_{22}^2 x + \gamma_2).$$

Daraus ergibt sich die Relation

$$(v_1 - v_2)(v_1 + v_2 + s_y) - u_1(v_{12}^2 x + \gamma_1) \equiv 0 \mod u_2.$$

Mit Hilfe des erweiterten euklidischen Algorithmus berechnet man $res_1 := \mathrm{ggt}(v_1 - v_2, u_2) \in k$ und $t_1 \in k[x]$ und mit

$$t_1(v_1 - v_2) \equiv res_1 \mod u_2.$$

Für den Rest r der euklidischen Division von $t_1 \cdot (u_1 - u_2)$ durch u_2 gilt somit

$$res_1 \cdot (v_1 + v_2 + s_y) - r \cdot (v_{12}^2 x + \gamma_1) + (r_2 \cdot v_{12}^2) \cdot u_2 = 0, \tag{3.13}$$

wobei $r = r_2 x^2 + r_1 x + r_0$.
Durch Koeffizientenvergleich sieht man leicht, dass

$$res_1 \cdot (v_{12} + v_{22}) - (r_2 \cdot \gamma_1) - (r_1 \cdot v_{12}^2) + (r_2 \cdot v_{12}^2) \cdot u_{22} = 0. \tag{3.14}$$

Da die Bestimmung von E_y unmittelbar zur Berechnung mindestens einer Inversion führt, betrachten wir

$$E := (res_1 \cdot r_2) \cdot E_y = (res_1 \cdot r_2) \cdot y^2 + s \cdot y + t, \quad t = t_3 x^3 + t_2 x^2 + t_1 x + t_0 \tag{3.15}$$

sowie

$$E_x := t_3^{-1} \cdot E =: k_1 \cdot y^2 + s_x \cdot y + t_x,$$

dabei ist $k_1 := t_3^{-1} \cdot (res_1 \cdot r_2)$ und t_x normiert. Dann gilt für die Resultante

$$Res_y(E, C) = k_1^3 \cdot \big(f \cdot \big(f + s_y \cdot (s_y^2 - 3t_y + h)\big) + h \cdot t_y \cdot (s_y^2 - 2t_y + h)\big) + t_x^3.$$

Der Leitkoeffizient von $Res_y(E, C)$ ist dann gegeben durch

$$A := 1 + k_1^3 \cdot h_3 \cdot t_{y_3} \cdot (-2t_{y_3} + h_3) = t_3^{-2} \cdot B$$

mit

$$B := t_3^2 + h_3 \cdot (-2t_3 \cdot (res_1 \cdot r_2) + h_3 \cdot (res_1 \cdot r_2)^2) = (t_3 - h_3 \cdot (res_1 \cdot r_2))^2.$$

Man beachte, dass im Falle $h_3 = 0$ die Resultante $Res_y(E, C)$ normiert ist. Andernfalls müssen wir B^{-1} berechnen, um $Res_y(E, C)$ zu normieren. Nun wie in (3.15) kann man E folgendermaßen darstellen

$$E = (res_1 \cdot r_2) \cdot (y - v_1) \cdot (y + v_1 + s_y) + u_1 \cdot ((res_1 \cdot r_2) \cdot v_{12}^2 x + \Gamma_1),$$

mit

$$\Gamma_1 = (res_1 \cdot r_2) \cdot \gamma_1.$$

Sei $\gamma_1' := \gamma_1 \cdot r_2 = \frac{\Gamma_1}{res_1}$. Nach (3.14) gilt dann

$$\gamma_1' = res_1 \cdot (v_{12} + v_{22}) - ((r_1 \cdot v_{12}^2) - (r_2 \cdot v_{12}^2) \cdot u_{22})$$

und

$$\Gamma_1 = res_1 \cdot \gamma_1'.$$

Multipliziert man (3.13) mit r_2, so erhält man

$$s = r \cdot ((r_2 \cdot v_{12}^2) \cdot x + \gamma_1') - (r_2 \cdot res_1) \cdot (v_1 + v_2) - r_2^2 \cdot v_{12}^2 \cdot u_2. \tag{3.16}$$

Mit der rechten Seite von (3.16) berechnet man $s(0)$ und $s(1)$ und somit auch

$$s = (s(1) - s(0))x + s(0) =: s_1 x + s_0.$$

Aus

$$t_y = -v_1 \cdot (v_1 + s_y) + u_1 \cdot (v_{12}^2 x + \gamma_1) \tag{3.17}$$

folgt nun

$$t = -v_1 \cdot ((res_1 \cdot r_2) \cdot v_1 + s) + u_1 \cdot (((res_1 \cdot r_2) \cdot v_{12}^2) \cdot x + \Gamma_1)$$

und durch Koeffizientenvergleich

$$t_3 = \Gamma_1 + u_{12} \cdot ((res_1 \cdot r_2) \cdot v_{12}^2) - v_{12} \cdot (s_1 + 2(res_1 \cdot r_2) \cdot v_{11}).$$

Wir berechnen wie erwähnt die simultane Inversion

$$inv := \begin{cases} (res_1 \cdot r_2 \cdot t_3)^{-1} & , \text{ falls } h_3 = 0 \\ (res_1 \cdot r_2 \cdot t_3 \cdot B)^{-1} & , \text{ falls } h_3 \neq 0. \end{cases}$$

Für $h_3 = 0$ erhält man dann

$$\begin{array}{lcl} (res_1 \cdot r_2)^{-1} & = & inv \cdot t_3 \\ k_1 & = & (res_1 \cdot r_2)^2 \cdot inv \end{array}$$

und für $h_3 \neq 0$

$$\begin{array}{lcl} (res_1 \cdot r_2 \cdot t_3)^{-1} & = & inv \cdot B \\ (res_1 \cdot r_2)^{-1} & = & (res_1 \cdot r_2 \cdot t_3)^{-1} \cdot t_3 \\ B^{-1} & = & (res_1 \cdot r_2 \cdot t_3) \cdot inv \\ k_1 & = & (res_1 \cdot r_2)^2 \cdot (res_1 \cdot r_2 \cdot t_3)^{-1}. \end{array}$$

Aus

$$\begin{array}{lcl} \gamma_1 & = & \Gamma_1 \cdot (res_1 \cdot r_2)^{-1} \\ s_y & = & (res_1 \cdot r_2)^{-1} \cdot s \end{array}$$

berechnet man t_y via (3.17) durch Interpolation an $0, 1, -1$ und ∞:

$$\begin{array}{rcl} t_y(0) & = & -v_{10}(v_{10} + s_{y0}) + u_{10}\gamma_1 \\ t_y(1) & = & -(v_{12} + v_{11} + v_{10})(v_{12} + v_{11} + v_{10} + s_{y1} + s_{y0}) \\ & & +(1 + u_{12} + u_{11} + u_{10})(v_{12}^2 + \gamma_1) \\ t_y(-1) & = & -(v_{12} - v_{11} + v_{10})(v_{12} - v_{11} + v_{10} - s_{y1} + s_{y0}) \\ & & +(-1 + u_{12} - u_{11} + u_{10})(-v_{12}^2 + \gamma_1) \\ t_y(\infty) & = & t_3(res_1 r_2)^{-1}. \end{array}$$

Somit ist auch t_x gegeben durch

$$t_x = k_1 \cdot t_y.$$

Da die Resultante $Res_y(E, C)$ in dem Algorithmus nur bei der Division durch ein normiertes Polynom vom Grad 6 verwendet wird, berechnen wir nur die ersten vier Koeffizienten der Resultante. Damit berechnet man nun

$$\begin{array}{lcl} H_1 & := & f(f + s_y(s_y^2 - 3t_y + h)) \\ H_2 & := & ht_y(s_y^2 - 2t_y + h) \end{array}$$

mittels Toom-Cook Multiplikation. Nun lässt sich auch das normierte Polynom $Res_y^*(E, C)$ mit A^{-1} berechnen:

$$Res_y^*(E, C) = A^{-1} \cdot (k_1^3 \cdot (H_1 + H_2) + t_x^3).$$

Der Rest der Berechnungen im Algorithmus 3 ist dann sehr leicht nachzuvollziehen: ein MAGMA Programm mit expliziten Formeln steht auf der folgende Webseite zur Verfügung:

`http://www.exp-math.uni-essen.de/~oyono`

Beispiel 3.2.2. Sei $\mathbb{F}_p$ der endliche Körper mit $p = 288230376151711813$ Elementen und C die Picard-Kurve mit der Gleichung

$$y^3 = x^4 + 211939155673366998x^2 + 180771375410752024x + 192949046001937542.$$

Mit der in [100] beschriebene Methode gelang es A. Weng die Anzahl der $\mathbb{F}_p$-rationalen Punkte $\#\mathrm{Jac}(C)(\mathbb{F}_p)$ zu berechnen

$$\#\mathrm{Jac}(C)(\mathbb{F}_p) = 23945242809810674383789064863599186983250020224864027,$$

welche eine 53 stellige Primzahl ist. Seien $D_1 = (u_1, v_1)$ und $D_2 = (u_2, v_2)$ mit

$$\begin{aligned}
u_1 &= x^3 + 45480416222142502x^2 + 25702135757197915 5x + 247897421008749706,\\
v_1 &= 249925361769859473x^2 + 65219164464402576x + 162437835874689870,\\
u_2 &= x^3 + 280541744851751366x^2 + 127975090148422907x + 212309834791637212,\\
v_2 &= 112253625856232562x^2 + 12407104324441326x + 159336746098327461.
\end{aligned}$$

Die Kubik E_1 durch D_1^+, D_2^+ und $3P^\infty$ besitzt die Gleichung

$$\begin{aligned}
E_1 = {} & y^2 + (69092631642129214x + 14205244030369094 2)y + 175568055651655894x^3\\
& +127429514908182064x^2 + 42674743031103393x + 193202666503167690,
\end{aligned}$$

und für $D_1 + D_2 = (u_3, v_3)$ gilt

$$\begin{aligned}
u_3 &= x^3 + 156166111541072953x^2 + 100784248633847721x + 166118752107432413,\\
v_3 &= 106068809090880054x^2 + 3061704980599997x + 192694500166962197.
\end{aligned}$$

Die Kubik E_2 durch $2D_1^+$ und $3P^\infty$ besitzt die Gleichung

$$\begin{aligned}
E_2 = {} & y^2 + (151020705062941714x + 71448245390763339)y + 212824123101073211x^3\\
& +190191236041983624x^2 + 16338465865018830x + 260362745413347034,
\end{aligned}$$

und für $2D_1 = (u_4, v_4)$ gilt

$$\begin{aligned}
u_4 &= x^3 + 131808142339003957x^2 + 54466261199795508x + 42479999828947478,\\
v_4 &= 27414077038443469x^2 + 160779982478686321x + 206554979228410844.
\end{aligned}$$

Anwendungen

In [78] beschreibt C. Ritzenthaler einen quasi-quadratischen Punktezählalgorithmus für nicht-hyperelliptische *ordinäre* Kurven $\tilde{C}$ vom Geschlecht 3 über $k = \mathbb{F}_{2^n}$.

Die vorgestellte AGM Methode berechnet das charakteristische Polynom des Frobenius bis auf Vorzeichen

$$\chi_{\tilde{C}}(\pm X).$$

Das Vorzeichen kann nun mittels der Arithmetik auf der Jacobischen sofort bestimmt werden.

Beispiel 3.2.3. Sei $\tilde{C}/k$ die glatte Quartik

$$(tx^2 + (t^3+1)y^2 + t^2z^2 + t^4xy + (t^3+t^2)xz + t^6yz)^2 - xyz(x+y+z) = 0,$$

wobei $k = \mathbb{F}_q$, $q = 2^N$ mit $N = 100$, und $t \neq 1$ ein Erzeuger von k mit $t^{101} - 1 = 0$ ist.
Auf die Rechner vom Typ `Opteron` 246 (1GHz) berechnet der in [78] beschriebene AGM-Algorithmus in 2 Minuten das Polynom $\chi_{\tilde{C}}(\pm X)$ bis auf Vorzeichen.

$$\begin{aligned}\chi_{\tilde{C}}(\pm X) = X^6 &+ 377276036264709 \cdot X^5 + 345535106116904583889422793740 3 \cdot X^4 \\ &+ 92979302197227669130776666646461687227769187 1 \cdot X^3 \\ &+ 345535106116904583889422793740 3 \cdot 2^{100} \cdot X^2 \\ &+ 377276036264709 \cdot 2^{200} \cdot X + 2^{300}.\end{aligned}$$

Mit dem von uns entworfenen Algorithmus bestimmen wir das richtige Vorzeichen von $\chi_{\tilde{C}}$. Die Berechnung (mitsamt der Erzeugung eines typischen Divisors) dauert etwa 4 Sekunden. Auf den gleichen Maschinen dauert die Verifizierung des Vorzeichens von $\chi_{\tilde{C}}$ mittels Magma's allgemeinen Algorithmen ca. 2 Minuten.

3.2.4 Fazit und Vergleich

Die folgende Tabelle liefert einen Vergleich zwischen der von uns vorgestellten Methode mit bereits existierenden Algorithmen zur Addition auf der Jacobischen von Geschlecht 3 Kurven. In den zwei ersten Zeilen fassen wir die Kosten unseres Algorithmus zusammen. Die Kurve C sei gegeben durch die affine Gleichung

$$y^3 + h(x)y = x^4 + f_2x^2 + f_1x + f_0.$$

Operationen		hyperelliptisch mit $g = 3$	C_{34}			generische Quartik
			Picard	$\deg(h_2) = 1$	$\deg(h_2) = 2$	$\deg(h_2) = 3$
Unsere	Add		2I+130M	2I+138M	2I+145M	2I+163M
Methode	Vdp		2I+152M	2I+160M	2I+167M	2I+185M
Methode	Add		2I+140M	2I+147M	2I+150M	
aus [6]	Vdp		2I+164M	2I+171M	2I+174M	
Methode	Add				5I+204M	
aus [2]	Vdp				5I+284M	
Methode	Add	I+70M				
aus [30]	Vdp	I+71M				

Die Methoden aus [2] und [6] entsprechen einer Verallgemeinerung des Algorithmus von Cantor. Es ist zu bemerken, dass die Methoden aus [2] und [6] bei Beginn dieser Dissertation noch nicht veröffentlicht waren. Zu diesem Zeitpunkt betrug die schnellste Reduktion (im Cantor'schen Algorithmus) zur Addition auf C_{34} Kurven $200M + 10I$ (siehe [6, section 6]).

Tabelle 3.1: **Addition,** $\deg u_1 = \deg u_2 = 3$

INPUT	$D_1 = (u_1, v_1)$ und $D_2 = (u_2, v_2)$ $u_i = x^3 + u_{i2}x^2 + u_{i1}x + u_{i0}, v_i = v_{i2}x^2 + v_{i1}x + v_{i0}$ $C : y^3 + h(x)y - f(x) = 0$ mit $h(x) := h_3x^3 + h_2x^2 + h_1x + h_0,\ f(x) := x^4 + f_2x^2 + f_1x + f_0$
OUTPUT	$D = \left(u_{D_1+D_2}, v_{D_1+D_2}\right) = D_1 + D_2$ mit $u_{D_1+D_2} = x^3 + u_2x^2 + u_1x + u_0$ $v_{D_1+D_2} = v_2x^2 + v_1x + v_0$

Step	Formeln	Kosten
1.1	Berechnung des Inversen t_1 von $v_1 - v_2$ modulo u_2 $a_1 = (v_{12}-v_{22})u_{22}-(v_{11}-v_{21}),a_2 = (v_{12}-v_{22})^2,a_3 = a_2u_{20}-a_1(v_{10}-v_{20});$ $a_4 = a_2(u_{22}+u_{21}+u_{20}+1)-(v_{12}-v_{22}+a_1)(v_{12}+v_{11}+v_{10}-(v_{22}+v_{21}+v_{20}))-a_3;$ $a_5 = a_4(v_{12}-v_{22}),a_6 = a_4(v_{11}-v_{21})-a_3(v_{12}-v_{22});$ $a_7 = a_4^2,res_1 = a_7(v_{10}-v_{20})-a_6a_3,t_{10} = a_1a_6,t_{12} = (v_{12}-v_{22})a_5;$ $t_{11} = (a_1+v_{12}-v_{22})(a_6+a_5)-(t_{10}+t_{12}),t_{10} = t_{10}+a_7;$ $t_1 = t_{12}x^2 + t_{11}x + t_{10}$	13M+2SQ
1.2	Berechnung des Restes r von $(u_1 - u_2)t_1$ durch u_2 $b_1 = (u_{12}+u_{11}+u_{10}-(u_{22}+u_{21}+u_{20}))(t_{12}+t_{11}+t_{10});$ $b_2 = (u_{12}-u_{11}+u_{10}-(u_{22}-u_{21}+u_{20}))(t_{12}-t_{11}+t_{10});$ $b_3 = (4(u_{12}-u_{22})+2(u_{11}-u_{21})+u_{10}-u_{20})(4t_{12}+2t_{11}+t_{10});$ $b_4 = (u_{12}-u_{22})t_{12},b_5 = (u_{10}-u_{20})t_{10},b_6 = (b_1+b_2)/2-(b_5+b_4);$ $b_7 = ((b_3+b_2-b_1-b_5)/2-2(4b_4+b_6))/3,b_8 = b_1-(b_5+b_6+b_7+b_4);$ $b_9 = b_7-b_4u_{22},r_2 = b_5-b_9u_{20};$ $b_{10} = b_4+b_7+b_6+b_8+b_5-(b_9+b_4)(u_{22}+u_{21}+u_{20}+1);$ $r_1 = (b_{10}-(b_4+b_6+b_5-(b_7+b_8)-(b_9-b_4)(u_{22}-u_{21}+u_{20}-1)))/2;$ $r_0 = b_{10}-(r_2+r_1);$ $r = r_0x^2 + r_1x + r_2$	9M
1.3	Berechnung der Kubik $E = y^2 + sy + t$ $c_1 = v_{12}^2,c_2 = r_0c_1,c_3 = res_1(v_{12}+v_{22})-(r_1c_1)+(c_2u_{22}),c_4 = c_3res_1;$ $c_5 = res_1r_0,c_6 = r_0c_2,,c_7 = r_2c_3-(c_6u_{20})-c_5(v_{10}+v_{20});$ $c_8 = (r_0+r_1+r_2)(c_2+c_3)-c_6(1+(u_{22}+u_{21}+u_{20}))-c_5(v_{22}+v_{21}+v_{20}+v_{12}+v_{11}+v_{10})-c_7;$ $c_9 = c_4+u_{12}c_5c_1-v_{12}(c_8+2c_5v_{11}),c_{10} = c_5c_9,c_{11} = c_5^2;$	39M+3SQ+I
$*_1$	$c_{12} = c_9^2,\ c_{13} = c_{12}+h_3(-2c_{10}+h_3c_{11}),\ inv_1 = (c_{10}c_{13})^{-1},\ c_{14} = c_{13}inv_1;$ $c_{15} = c_9c_{14},\ c_{16} = c_{12}inv_1c_{10};$	(7M+SQ+I)
	$s_0 = c_7c_{15},\ s_1 = c_8c_{15},\ c_{17} = c_4c_{15};$ $c_{18} = (1+u_{12}+u_{11}+u_{10})(c_1+c_{17})-(v_{12}+v_{11}+v_{10})(v_{12}+v_{11}+v_{10}+s_1+s_0);$ $t_3 = c_9c_{15},\ t_0 = u_{10}c_{17}-v_{10}(v_{10}+s_0);$ $t_2 = (c_{18}+(-1+u_{12}-u_{11}+u_{10})(-c_1+c_{17})-(v_{12}-v_{11}+v_{10})(v_{12}-v_{11}+v_{10}-s_1+s_0))/2-t_0;$ $t_1 = c_{18}-(t_0+t_2+t_3),\ k_1 = c_{11}c_{14},\ c_{19} = t_0k_1,\ c_{20} = t_1k_1,\ c_{21} = t_2k_1;$ $E = y^2 + (s_1x+s_0)y + t_3x^3 + t_2x^2 + t_1x + t_0$	
2.1	Berechnung von $res_y(E,C)$ und $\tilde{u} := res_y(E,C)^*/(u_1u_2)$ $d_0 = c_{21}^2,\ d_1 = 3c_{21},\ d_2 = 3(c_{20}+d_0),\ d_3 = c_{21}(6c_{20}+d_0)+3c_{19};$ $d_4 = s_1^2,\ d_5 = s_0^2,\ d_6 = (s_1+s_0)^2-(d_4+d_5),\ d_7 = (s_1+s_0)(t_3+t_2+t_1+t_0);$ $d_8 = (s_0-s_1)(t_2+t_0-(t_3+t_1)),\ d_9 = (2s_1+s_0)(8t_3+4t_2+2t_1+t_0);$ $d_{10} = s_1t_3,\ d_{11} = s_0t_0,\ d_{12} = -(d_{11}+d_{10})+(d_7+d_8)/2;$ $d_{13} = -2d_{10}+(d_{11}-d_7+(d_9-d_8)/3)/2,\ d_{14} = d_7-(d_{11}+d_{12}+d_{13}+d_{10});$ $d_{15} = s_1d_4,\ d_{16} = 3d_4s_0,\ d_{17} = 1-3d_{10},\ d_{18} = d_{15}-3d_{13};$ $d_{19} = f_2+d_{16}+(1-3d_{10})f_2-3d_{12};$	37M+5SQ
$*_2$	$d_{20} = (t_3+t_2+t_1+t_0)(h_3+h_2+h_1+h_0+d_4+d_6+d_5-2(t_3+t_2+t_1+t_0));$ $d_{21} = (-t_3+t_2-t_1+t_0)(2(t_3-t_2+t_1-t_0)-h_3+h_2-h_1+h_0+d_4-d_6+d_5);$ $d_{22} = (8t_3+4t_2+2t_1+t_0)(8(-2t_3+h_3)+4(d_4-2t_2+h_2)+2(d_6-2t_1+h_1)+d_5-2t_0+h_0);$	(15M)

	$d_{23} = (-8t_3 + 4t_2 - 2t_1 + t_0)(-8(-2t_3 + h_3) + 4(d_4 - 2t_2 + h_2) - 2(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0)$; $d_{24} = (27t_3 + 9t_2 + 3t_1 + t_0)(27(-2t_3 + h_3) + 9(d_4 - 2t_2 + h_2) + 3(d_6 - 2t_1 + h_1) + d_5 - 2t_0 + h_0)$; $d_{25} = t_0(d_5 - 2t_0 + h_0)$, $d_{26} = t_3(-2t_3 + h_3)$,$d_{32} = f_2 s_1$; $d_{27} = -5d_{26} + ((-(d_{20} + d_{21}) + (3d_{25} + (d_{23} + d_{22})/2)/2)/2)/3$; $d_{28} = 15d_{26} + (((5d_{25} - 7d_{20} + (-d_{24} + 7d_{22} - d_{23} - d_{21})/2)/2)/2)/3$; $d_{29} = -3d_{26} + (((d_{20} - d_{25} + (d_{21} - d_{22} + (d_{24} - d_{23})/5)/2)/2)/2)/3$; $d_{33} = (h_3 + h_2 + h_1 + h_0)(d_{26} + d_{29} + d_{27} + d_{28} + s_1 + s_0 + d_{32})$; $d_{34} = (-h_3 + h_2 - h_1 + h_0)(-d_{26} + d_{29} - d_{27} + d_{28} + s_1 - s_0 + d_{32})$; $d_{35} = (8h_3 + 4h_2 + 2h_1 + h_0)(8d_{26} + 4(d_{29} + s_1) + 2(d_{27} + s_0) + d_{28} + d_{32})$; $d_{36} = (-8h_3 + 4h_2 - 2h_1 + h_0)(-8d_{26} + 4(d_{29} + s_1) - 2(d_{27} + s_0) + d_{28} + d_{32})$; $d_{37} = (27h_3 + 9h_2 + 3h_1 + h_0)(27d_{26} + 9(d_{29} + s_1) + 3(d_{27} + s_0) + d_{28} + d_{32})$; $d_{38} = h_0(d_{28} + d_{32})$, $d_{44} = h_3 d_{26}$; $d_{42} = -5d_{44} + ((-(d_{33} + d_{34}) + (3d_{38} + (d_{36} + d_{35})/2)/2)/2)/3$; $d_{41} = 15d_{44} + (((5d_{38} - 7d_{33} + (-d_{37} + 7d_{35} - d_{36} - d_{34})/2)/2)/2)/3$; $d_{43} = -3d_{44} + (((d_{33} - d_{38} + (d_{34} - d_{35} + (d_{37} - d_{36})/5)/2)/2)/2)/3$; $d_{40} = (d_{33} + d_{34})/2 - (d_{38} + d_{42} + d_{44})$; $d_{39} = d_{33} - (d_{38} + d_{40} + d_{41} + d_{42} + d_{43} + d_{44})$;	
	$d_{45} = k_1^3$, $d_{46} = d_{45}(d_{19} + d_{41}) + d_3$, $d_{47} = d_{45}(d_{18} + d_{42}) + d_2$; $d_{48} = d_{45}(d_{17} + d_{43}) + d_1$;	
$*_3$	$d_{46} = d_{46}c_{16}$, $d_{47} = d_{47}c_{16}$, $d_{48} = d_{48}c_{16}$;	(3M)
	$d_{49} = u_{12} + u_{22}$, $d_{50} = u_{21} + u_{11} + u_{12}u_{22}$; $d_{51} = u_{20} + u_{10} + u_{12}u_{21} + u_{11}u_{22}$, $u_2' = d_{48} - d_{49}$; $u_1' = d_{47} - d_{50} - d_{49}u_2'$, $u_0' = -d_{49}u_1' + d_{46} - d_{51} - d_{50}(d_{48} - d_{49})$; $\tilde{u} = x^3 + u_2'x^2 + u_1'x + u_0'$	
2.2	Berechnung des Inversen α_1 von $t - s^2 - h$ modulo $\tilde{u}$ $g_1 = t_3 - h_3$, $g_0 = g_1(1 + u_2' + u_1' + u_0')$, $g_2 = t_0 - (d_5 + h_0 + g_1u_0')$; $g_3 = t_3 + t_2 + t_1 + t_0 - (h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 + g_0)$; $g_5 = (t_3 + t_2 + t_1 + t_0 - (h_3 + h_2 + h_1 + h_0 + d_4 + d_6 + d_5 + g_0) - (-t_3 + t_2 - t_1 + t_0 + h_3 - h_2 + h_1 - h_0 - d_4 + d_6 - d_5 - g_1(-1 + u_2' - u_1' + u_0')))/2$; $g_6 = g_3 - g_5 - g_2$, $g_7 = g_6u_2' - g_5$, $g_8 = g_6^2$, $g_{10} = g_8u_0' - g_7g_2$; $g_{11} = g_8(1 + u_2' + u_1' + u_0') - (g_6 + g_7)(g_6 + g_5 + g_2) - g_{10}$, $g_{12} = g_{11}g_6$; $g_{13} = g_{11}g_5 - g_{10}g_6$, $g_9 = g_{11}^2$, $res_2 = g_9g_2 - g_{13}g_{10}$,$\alpha_{10} = g_7g_{13}$; $\alpha_{12} = g_6g_{12}$,$\alpha_{11} = (g_6 + g_7)(g_{12} + g_{13}) - \alpha_{10} - \alpha_{12}$, $\alpha_{10} = \alpha_{10} + g_9$; $\alpha_1 = \alpha_{12}x^2 + \alpha_{11}x + \alpha_{10}$	16M+2SQ
2.3	Berechnung des Restes v von $\alpha_1(st - f)$ durch $\tilde{u}$ $i_1 = d_{10} - 1$, $i_2 = d_{13} - (d_{10} - 1)u_2'$, $i_3 = d_{11} - f_0 - i_2u_0'$; $i_4 = d_{10} + d_{13} + d_{12} + d_{14} + d_{11} - (1 + f_2 + f_1 + f_0) - (i_2 + i_1)(u_2' + u_1' + u_0' + 1)$; $i_5 = (i_4 - ((d_{10} - d_{13} + d_{12} - d_{14} + d_{11} - 1 - f_2 + f_1 - f_0) - (i_2 - i_1)(u_2' - u_1' + u_0' - 1)))/2$; $i_6 = i_4 - i_3 - i_5$, $i_7 = (i_6 + i_5 + i_3)(\alpha_{12} + \alpha_{11} + \alpha_{10})$, $i_9 = i_6\alpha_{12}$, $i_{10} = i_3\alpha_{10}$; $i_8 = (i_6 - i_5 + i_3)(\alpha_{12} - \alpha_{11} + \alpha_{10})$, ,$i_{11} = (i_7 + i_8)/2 - (i_{10} + i_9)$; $i_{12} = (((4i_6 + 2i_5 + i_3)(4\alpha_{12} + 2\alpha_{11} + \alpha_{10}) - i_7 + i_8 - i_{10})/2 - 2(4i_9 + i_{11}))/3$; $i_{13} = i_7 - (i_{10} + i_{11} + i_{12} + i_9)$, $i_{14} = i_9$, $i_{15} = i_{12} - i_9u_2'$, $i_{16} = i_{10} - i_{15}u_0'$; $i_{17} = (i_9 + i_{12} + i_{11} + i_{13} + i_{10}) - (i_{15} + i_{14})(u_2' + u_1' + u_0' + 1)$; $i_{18} = (i_{17} - (i_9 - i_{12} + i_{11} - i_{13} + i_{10}) + (i_{15} - i_{14})(u_2' - u_1' + u_0' - 1))/2$; $i_{19} = i_{17} - i_{16} - i_{18}$, $inv_2 = (res_2i_{19})^{-1}$, $i_{20} = inv_2i_{19}$; $v_0 = i_{20}i_{16}$, $v_1 = i_{20}i_{18}$, $v_2 = i_{20}i_{19}$; $v = v_2x^2 + v_1x + v_0$	18M+I
3	Berechnung von $u := u_{D_1+D_2}$ $j_1 = inv_2res_2^2$, $j_2 = j_1^3$, $j_3 = j_1v_1$, $j_4 = j_3^2$, $j_5 = j_1v_0$, $j_6 = j_3(j_4 + 6j_5)$;	16M+3SQ
$*_4$	$j_7 = (v_2 + v_1 + v_0)(h_3 + h_2 + h_1)$, $j_8 = (v_2 - v_1 + v_0)(h_3 - h_2 + h_1)$, $j_9 = v_2h_3$; $j_{10} = v_0h_1$,$j_{11} = (j_7 + j_8)/2 - (j_{10} + j_9)$, $j_{12} = 3j_3 + j_2j_9$, $j_{14} = j_6 + j_2j_{11}$; $j_{13} = 3(j_5 + j_4) - j_2 + j_2((((4v_2 + 2v_1 + v_0)(4h_3 + 2h_2 + h_1) - j_7 + j_8 - j_{10})/2 - 2(4j_9 + j_{11}))/3)$;	(8M)
	$u_2 = j_{12} - u_2'$, $u_1 = j_{13} - u_1' - u_2'u_2$, $u_0 = -u_2'u_1 + j_{14} - u_0' - u_1'(j_{12} - u_2')$; $u = x^3 + u_2x^2 + u_1x + u_0$	
total		148M, 15SQ, 2I

Tabelle 3.2: **Verdopplung,** $\deg u_1 = 3$

INPUT	$D_1 = (u_1, v_1)$ $u_1 = x^3 + u_{12}x^2 + u_{11}x + u_{10},\ v_1 = v_{12}x^2 + v_{11}x + v_{10}$ $C : y^3 + h(x)y - f(x) = 0$ mit $h(x) := h_3x^3 + h_2x^2 + h_1x + h_0,\ f(x) := x^4 + f_2x^2 + f_1x + f_0$
OUTPUT	$D = \left(u_{2D_1}, v_{2D_1}\right) = 2D_1$ mit $u_{2D_1} = x^3 + u_2x^2 + u_1x + u_0$ $v_{2D_1} = v_2x^2 + v_1x + v_0$

Step	Formeln	Kosten
1.1	Berechnung von w_1 mit $u_1w_1 = v_1^3 + h(x)v_1 - f(x)$ $l_1 = (v_{12} + v_{11} + v_{10})^2$, $l_2 = (v_{12} - v_{11} + v_{10})^2$, $l_3 = v_{12}^2$, $l_4 = v_{10}^2$; $l_5 = (l_1 + l_2)/2 - (l_4 + l_3)$; $l_6 = (((4v_{12} + 2v_{11} + v_{10})^2 - l_1 + l_2 - l_4)/2 - 2(4l_3 + l_5))/3$; $l_7 = l_1 - (l_4 + l_5 + l_6 + l_3)$,$l_8 = (v_{12} + v_{11} + v_{10})(l_3 + l_6 + l_5 + l_7 + h_3 + h_2 + h_1)$; $l_9 = (v_{12} - v_{11} + v_{10})(-l_3 + l_6 + h_3 - (l_5 + h_2) + l_7 + h_1)$; $l_{10} = (4v_{12} + 2v_{11} + v_{10})(8l_3 + 4(l_6 + h_3) + 2(l_5 + h_2) + l_7 + h_1)$; $l_{11} = (4v_{12} - 2v_{11} + v_{10})(-8l_3 + 4(l_6 + h_3) - 2(l_5 + h_2) + l_7 + h_1)$; $l_{12} = v_{10}(l_7 + h_1)$, $l_{13} = v_{12}l_3$,$l_{14} = -5l_{13} + ((l_9 - l_8 + (l_{10} - l_{11})/2)/2)/3$; $l_{15} = ((-(l_8 + l_9) + (3l_{12} + (l_{10} + l_{11})/2)/2)/2)/3$; $l_{16} = (l_8 + l_9)/2 - (l_{12} + l_{15})$,$l_{14} = l_{14} - 1$,$w_{13} = l_{13}$,$w_{12} = l_{15} - w_{13}u_{12}$; $w_{11} = l_{14} - w_{13}u_{11} - w_{12}u_{12}$,$w_{10} = l_{16} - w_{13}u_{10} - w_{12}u_{11} - w_{11}u_{12}$; $w_1 = w_{13}x^3 + w_{12}x^2 + w_{11}x + w_{10}$	12M+5SQ
1.2	Berechnung des Inversen t_1 von w_1 modulo u_1 $a_1 = w_{13}$, $a_2 = w_{10} - a_1u_{10}$; $a_3 = w_{13} + w_{12} + w_{11} + w_{10} - a_1(1 + u_{12} + u_{11} + u_{10})$; $a_4 = (a_3 - (-w_{13} + w_{12} - w_{11} + w_{10} - a_1(-1 + u_{12} - u_{11} + u_{10})))/2$; $a_5 = a_3 - a_4 - a_2$, $a_6 = a_5u_{12} - a_4$, $a_7 = a_5^2$, $a_8 = a_7u_{10} - a_6a_2$; $a_9 = a_7(1 + u_{12} + u_{11} + u_{10}) - (a_5 + a_6)(a_5 + a_4 + a_2) - a_8$, $a_{10} = a_9a_5$; $a_{11} = a_9a_4 - a_8a_5$, $a_7 = a_9^2$, $res_1 = a_7a_2 - a_{11}a_8$, $t_{10} = a_6a_{11}$; $t_{12} = a_5a_{10}$, $t_{11} = (a_5 + a_6)(a_{10} + a_{11}) - t_{10} - t_{12}$, $t_{10} = t_{10} + a_7$; $t_1 = t_{12}x^2 + t_{11}x + t_{10}$	16M+2SQ
1.3	Berechnung des Restes r von $(3v_1^2 + h)t_1$ durch u_1 $b_1 = 3l_6 + h_3 - 3l_3u_{12}$, $b_2 = 3l_4 + h_0 - b_1u_{10}$; $b_3 = (3l_3 + 3l_6 + h_3 + 3l_5 + h_2 + 3l_7 + h_1 + 3l_4 + h_0) - (b_1 + 3l_3)(u_{12} + u_{11} + u_{10} + 1)$; $b_4 = (b_3 - ((3l_3 - (3l_6 + h_3) + 3l_5 + h_2 - (3l_7 + h_1) + 3l_4 + h_0) - (b_1 - 3l_3)(u_{12} - u_{11} + u_{10} - 1)))/2$; $b_5 = b_3 - b_2 - b_4$, $b_6 = (b_5 + b_4 + b_2)(t_{12} + t_{11} + t_{10})$; $b_7 = (b_5 - b_4 + b_2)(t_{12} - t_{11} + t_{10})$, $b_8 = b_5t_{12}$, $b_9 = b_2t_{10}$; $b_{10} = (b_6 + b_7)/2 - (b_9 + b_8)$; $b_{11} = (((4b_5 + 2b_4 + b_2)(4t_{12} + 2t_{11} + t_{10}) - b_6 + b_7 - b_9)/2 - 2(4b_8 + b_{10}))/3$; $b_{12} = b_6 - (b_9 + b_{10} + b_{11} + b_8)$, $b_{13} = b_{11} - b_8u_{12}$, $r_2 = b_9 - b_{13}u_{10}$; $b_{14} = (b_8 + b_{11} + b_{10} + b_{12} + b_9) - (b_{13} + b_8)(u_{12} + u_{11} + u_{10} + 1)$; $r_1 = (b_{14} - (b_8 + b_{10} + b_9) + (b_{11} + b_{12}) + (b_{13} - b_8)(u_{12} - u_{11} + u_{10} - 1))/2$; $r_0 = b_{14} - (r_2 + r_1)$; $r = r_0x^2 + r_1x + r_2$	13M
1.4	Berechnung der Kubik $E = y^2 + sy + t$ $c_1 = l_3$, $c_2 = r_0c_1$, $c_3 = 2res_1v_{12} - (r_1c_1 - c_2u_{12})$, $c_4 = c_3res_1$, $c_5 = res_1r_0$; $c_6 = r_0c_2$, $c_7 = r_2c_3 - c_6u_{10} - 2c_5v_{10}$; $c_8 = (r_0 + r_1 + r_2)(c_2 + c_3) - c_6(1 + u_{12} + u_{11} + u_{10}) - 2c_5(v_{12} + v_{11} + v_{10}) - c_7$; $c_9 = c_4 + u_{12}c_5c_1 - v_{12}(c_8 + 2c_5v_{11})$, $c_{10} = c_5c_9$, $c_{11} = c_5^2$;	39M+2SQ+I
$*_1$	$c_{12} = c_9^2$, $c_{13} = c_{12} + h_3(-2c_{10} + h_3c_{11})$, $inv_1 = (c_{10}c_{13})^{-1}$, $c_{14} = c_{13}inv_1$; $c_{15} = c_9c_{14}$, $c_{16} = c_{12}inv_1c_{10}$;	(7M+SQ+I)
	$s_0 = c_7c_{15}$, $s_1 = c_8c_{15}$, $c_{17} = c_4c_{15}$; $c_{18} = (1 + u_{12} + u_{11} + u_{10})(c_1 + c_{17}) - (v_{12} + v_{11} + v_{10})(v_{12} + v_{11} + v_{10} + s_1 + s_0)$; $t_3 = c_9c_{15}$, $t_0 = u_{10}c_{17} - v_{10}(v_{10} + s_0)$; $t_2 = (c_{18} + (-1 + u_{12} - u_{11} + u_{10})(-c_1 + c_{17}) - (v_{12} - v_{11} + v_{10})(v_{12} - v_{11} + v_{10} - s_1 + s_0))/2 - t_0$; $t_1 = c_{18} - (t_0 + t_2 + t_3)$, $k_1 = c_{11}c_{14}$, $c_{19} = t_0k_1$, $c_{20} = t_1k_1$, $c_{21} = t_2k_1$; $E = y^2 + (s_1x + s_0)y + t_3x^3 + t_2x^2 + t_1x + t_0$	

2.1	Berechnung von $res_y(E,C)$ und $\tilde{u} := res_y(E,C)^*/(u_1u_2)$ $d_0 = c_{21}^2$, $d_1 = 3c_{21}$, $d_2 = 3(c_{20}+d_0)$, $d_3 = c_{21}(6c_{20}+d_0)+3c_{19}$; $d_4 = s_1^2$, $d_5 = s_0^2$, $d_6 = (s_1+s_0)^2-(d_4+d_5)$, $d_7 = (s_1+s_0)(t_3+t_2+t_1+t_0)$; $d_8 = (s_0-s_1)(t_2+t_0-(t_3+t_1))$, $d_9 = (2s_1+s_0)(8t_3+4t_2+2t_1+t_0)$; $d_{10} = s_1t_3$, $d_{11} = s_0t_0$, $d_{12} = -(d_{11}+d_{10})+(d_7+d_8)/2$; $d_{13} = -2d_{10}+(d_{11}-d_7+(d_9-d_8)/3)/2$, $d_{14} = d_7-(d_{11}+d_{12}+d_{13}+d_{10})$; $d_{15} = s_1d_4$, $d_{16} = 3d_4s_0$, $d_{17} = 1-3d_{10}$, $d_{18} = d_{15}-3d_{13}$; $d_{19} = f_2+d_{16}+(1-3d_{10})f_2-3d_{12}$;	35M+6SQ
$*_2$	$d_{20} = (t_3+t_2+t_1+t_0)(h_3+h_2+h_1+h_0+d_4+d_6+d_5-2(t_3+t_2+t_1+t_0))$; $d_{21} = (-t_3+t_2-t_1+t_0)(2(t_3-t_2+t_1-t_0)-h_3+h_2-h_1+h_0+d_4-d_6+d_5)$; $d_{22} = (8t_3+4t_2+2t_1+t_0)(8(-2t_3+h_3)+4(d_4-2t_2+h_2)+2(d_6-2t_1+h_1)+d_5-2t_0+h_0)$; $d_{23} = (-8t_3+4t_2-2t_1+t_0)(-8(-2t_3+h_3)+4(d_4-2t_2+h_2)-2(d_6-2t_1+h_1)+d_5-2t_0+h_0)$; $d_{24} = (27t_3+9t_2+3t_1+t_0)(27(-2t_3+h_3)+9(d_4-2t_2+h_2)+3(d_6-2t_1+h_1)+d_5-2t_0+h_0)$; $d_{25} = t_0(d_5-2t_0+h_0)$, $d_{26} = t_3(-2t_3+h_3)$,$d_{32} = f_2s_1$; $d_{27} = -5d_{26}+((-(d_{20}+d_{21})+(3d_{25}+(d_{23}+d_{22})/2)/2)/2)/3$; $d_{28} = 15d_{26}+(((5d_{25}-7d_{20}+(-d_{24}+7d_{22}-d_{23}-d_{21})/2)/2)/2)/3$; $d_{29} = -3d_{26}+(((d_{20}-d_{25}+(d_{21}-d_{22}+(d_{24}-d_{23})/5)/2)/2)/2)/3$; $d_{33} = (h_3+h_2+h_1+h_0)(d_{26}+d_{29}+d_{27}+d_{28}+s_1+s_0+d_{32})$; $d_{34} = (-h_3+h_2-h_1+h_0)(-d_{26}+d_{29}-d_{27}+d_{28}+s_1-s_0+d_{32})$; $d_{35} = (8h_3+4h_2+2h_1+h_0)(8d_{26}+4(d_{29}+s_1)+2(d_{27}+s_0)+d_{28}+d_{32})$; $d_{36} = (-8h_3+4h_2-2h_1+h_0)(-8d_{26}+4(d_{29}+s_1)-2(d_{27}+s_0)+d_{28}+d_{32})$; $d_{37} = (27h_3+9h_2+3h_1+h_0)(27d_{26}+9(d_{29}+s_1)+3(d_{27}+s_0)+d_{28}+d_{32})$; $d_{38} = h_0(d_{28}+d_{32})$, $d_{44} = h_3d_{26}$; $d_{42} = -5d_{44}+((-(d_{33}+d_{34})+(3d_{38}+(d_{36}+d_{35})/2)/2)/2)/3$; $d_{41} = 15d_{44}+(((5d_{38}-7d_{33}+(-d_{37}+7d_{35}-d_{36}-d_{34})/2)/2)/2)/3$; $d_{43} = -3d_{44}+(((d_{33}-d_{38}+(d_{34}-d_{35}+(d_{37}-d_{36})/5)/2)/2)/2)/3$; $d_{40} = (d_{33}+d_{34})/2-(d_{38}+d_{42}+d_{44})$; $d_{39} = d_{33}-(d_{38}+d_{40}+d_{41}+d_{42}+d_{43}+d_{44})$;	(15M)
	$d_{45} = k_1^3$, $d_{46} = d_{45}(d_{19}+d_{41})+d_3$, $d_{47} = d_{45}(d_{18}+d_{42})+d_2$; $d_{48} = d_{45}(d_{17}+d_{43})+d_1$;	
$*_3$	$d_{46} = d_{46}c_{16}$, $d_{47} = d_{47}c_{16}$, $d_{48} = d_{48}c_{16}$;	(3M)
	$d_{49} = 2u_{12}$, $d_{50} = 2u_{11}+u_{12}^2$, $d_{51} = 2u_{10}+2u_{12}u_{11}$, $u_2' = d_{48}-d_{49}$; $u_1' = d_{47}-d_{50}-d_{49}u_2'$, $u_0' = -d_{49}u_1'+d_{46}-d_{51}-d_{50}(d_{48}-d_{49})$; $\tilde{u} = x^3+u_2'x^2+u_1'x+u_0'$	
2.2	Berechnung des Inversen α_1 von $t-s^2-h$ modulo $\tilde{u}$ $g_1 = t_3-h_3$,$g_0 = g_1(1+u_2'+u_1'+u_0')$, $g_2 = t_0-(d_5+h_0+g_1u_0')$; $g_3 = t_3+t_2+t_1+t_0-(h_3+h_2+h_1+h_0+d_4+d_6+d_5+g_0)$; $g_5 = (t_3+t_2+t_1+t_0-(h_3+h_2+h_1+h_0+d_4+d_6+d_5+g_0)-(-t_3+t_2-t_1+t_0+h_3-h_2+h_1-h_0-d_4+d_6-d_5-g_1(-1+u_2'-u_1'+u_0')))/2$; $g_6 = g_3-g_5-g_2$, $g_7 = g_6u_2'-g_5$, $g_8 = g_6^2$, $g_{10} = g_8u_0'-g_7g_2$; $g_{11} = g_8(1+u_2'+u_1'+u_0')-(g_6+g_7)(g_6+g_5+g_2)-g_{10}$, $g_{12} = g_{11}g_6$; $g_{13} = g_{11}g_5-g_{10}g_6$, $g_9 = g_{11}^2$, $res_2 = g_9g_2-g_{13}g_{10}$,$\alpha_{10} = g_7g_{13}$; $\alpha_{12} = g_6g_{12}$,$\alpha_{11} = (g_6+g_7)(g_{12}+g_{13})-\alpha_{10}-\alpha_{12}$, $\alpha_{10} = \alpha_{10}+g_9$; $\alpha_1 = \alpha_{12}x^2+\alpha_{11}x+\alpha_{10}$	16M+2SQ
2.3	Berechnung des Restes v von $\alpha_1(st-f)$ durch $\tilde{u}$ $i_1 = d_{10}-1$, $i_2 = d_{13}-(d_{10}-1)u_2'$, $i_3 = d_{11}-f_0-i_2u_0'$; $i_4 = d_{10}+d_{13}+d_{12}+d_{14}+d_{11}-(1+f_2+f_1+f_0)-(i_2+i_1)(u_2'+u_1'+u_0'+1)$; $i_5 = (i_4-((d_{10}-d_{13}+d_{12}-d_{14}+d_{11}-1-f_2+f_1-f_0)-(i_2-i_1)(u_2'-u_1'+u_0'-1)))/2$; $i_6 = i_4-i_3-i_5$, $i_7 = (i_6+i_5+i_3)(\alpha_{12}+\alpha_{11}+\alpha_{10})$, $i_9 = i_6\alpha_{12}$, $i_{10} = i_3\alpha_{10}$; $i_8 = (i_6-i_5+i_3)(\alpha_{12}-\alpha_{11}+\alpha_{10})$, ,$i_{11} = (i_7+i_8)/2-(i_{10}+i_9)$; $i_{12} = (((4i_6+2i_5+i_3)(4\alpha_{12}+2\alpha_{11}+\alpha_{10})-i_7+i_8-i_{10})/2-2(4i_9+i_{11}))/3$; $i_{13} = i_7-(i_{10}+i_{11}+i_{12}+i_9)$, $i_{14} = i_9$, $i_{15} = i_{12}-i_9u_2'$, $i_{16} = i_{10}-i_{15}u_0'$; $i_{17} = (i_9+i_{12}+i_{11}+i_{13}+i_{10})-(i_{15}+i_{14})(u_2'+u_1'+u_0'+1)$; $i_{18} = (i_{17}-(i_9-i_{12}+i_{11}-i_{13}+i_{10})+(i_{15}-i_{14})(u_2'-u_1'+u_0'-1))/2$; $i_{19} = i_{17}-i_{16}-i_{18}$, $inv_2 = (res_2i_{19})^{-1}$, $i_{20} = inv_2i_{19}$; $v_0 = i_{20}i_{16}$, $v_1 = i_{20}i_{18}$, $v_2 = i_{20}i_{19}$; $v = v_2x^2+v_1x+v_0$	18M+I

3	Berechnung von $u := u_{2D_1}$ $j_1 = inv_2 res_2^2$, $j_2 = j_1^3$, $j_3 = j_1 v_1$, $j_4 = j_3^2$, $j_5 = j_1 v_0$, $j_6 = j_3(j_4 + 6j_5)$;	16M+3SQ
$*_4$	$j_7 = (v_2+v_1+v_0)(h_3+h_2+h_1)$, $j_8 = (v_2-v_1+v_0)(h_3-h_2+h_1)$, $j_9 = v_2 h_3$; $j_{10} = v_0 h_1$,$j_{11} = (j_7 + j_8)/2 - (j_{10} + j_9)$, $j_{12} = 3j_3 + j_2 j_9$, $j_{14} = j_6 + j_2 j_{11}$; $j_{13} = 3(j_5 + j_4) - j_2 + j_2((((4v_2 + 2v_1 + v_0)(4h_3 + 2h_2 + h_1) - j_7 + j_8 - j_{10})/2 - 2(4j_9 + j_{11}))/3)$;	(8M)
	$u_2 = j_{12} - u_2'$, $u_1 = j_{13} - u_1' - u_2' u_2$, $u_0 = -u_2' u_1 + j_{14} - u_0' - u_1'(j_{12} - u_2')$; $u = x^3 + u_2 x^2 + u_1 x + u_0$	
total		165M, 20SQ, 2I

Tabelle 3.3: Falls $h_3 = 0$, ersetze $*_1, *_2, *_3$ und $*_4$ durch

$*_1$	$inv_1 = c_{10}^{-1}$,$c_{14} = inv_1$,$c_{15} = inv_1 c_9$,$c_{16} = 1$;	(M+I)
$*_2$	$d_{27} = (t_3 + t_2 + t_1)(h_1 + h_2 + d_4 + d_6 - 2(t_3 + t_2 + t_1))$; $d_{28} = (t_3 - t_2 + t_1)(h_1 - h_2 + d_6 - d_4 - 2(t_3 - t_2 + t_1))$; $d_{29} = (4t_3 + 2t_2 + t_1)(-8t_3 + 2(d_4 - 2t_2 + h_2) + d_6 - 2t_1 + h_1)$; $d_{30} = -2t_3^2$,$d_{31} = t_1(d_6 - 2t_1 + h_1)$,$d_{32} = (d_{27} + d_{28})/2 - (d_{31} + d_{30})$; $d_{33} = ((d_{29} - d_{27} + d_{28} - d_{31})/2 - 2(4d_{30} + d_{32}))/3$; $d_{35} = (h_2 + h_1 + h_0)(d_{30} + d_{33} + d_{32} + s_0 + s_1)$; $d_{36} = (h_2 - h_1 + h_0)(d_{30} - d_{33} + d_{32} + s_0 - s_1)$; $d_{37} = (4h_2 + 2h_1 + h_0)(4d_{30} + 2(d_{33} + s_1) + d_{32} + s_0)$; $d_{43} = h_2 d_{30}$,$d_{39} = h_0(d_{32} + s_0)$,$d_{41} = (d_{35} + d_{36})/2 - (d_{39} + d_{43})$; $d_{42} = ((d_{37} - d_{35} + d_{36} - d_{39})/2 - 2(4d_{43} + d_{41}))/3$; $d_{40} = d_{35} - (d_{39} + d_{41} + d_{42} + d_{43})$,$d_{44} = 0$;	(9M+SQ)
$*_3$		
$*_4$	$j_{11} = v_2 h_2$,$j_{12} = 3j_3$,$j_{13} = 3(j_5 + j_4) - j_2 + j_2 j_{11}$; $j_{14} = j_6 + j_2((v_2 + v_1)(h_2 + h_1) - (v_1 h_1 + j_{11}))$;	(5M)

Tabelle 3.4: Falls $h_3, h_2 = 0$, ersetze $*_1, *_2, *_3$ und $*_4$ durch

$*_1$	$inv_1 = c_{10}^{-1}$,$c_{14} = inv_1$,$c_{15} = inv_1 c_9$,$c_{16} = 1$;	(M+I)
$*_2$	$d_{37} = -2t_3^2$,$d_{35} = t_2(d_4 - 2t_2)$,$d_{38} = 0$,$d_{39} = 0$,$d_{43} = 0$,$d_{44} = 0$; $d_{36} = (t_3 + t_2)(d_4 - 2(t_3 + t_2)) - (d_{35} + d_{37})$,$d_{42} = h_1 d_{37}$,$d_{40} = h_0(d_{36} + s_1)$; $d_{41} = (h_1 + h_0)(d_{37} + d_{36} + s_1) - (d_{40} + d_{42})$;	(5M+SQ)
$*_3$		
$*_4$	$j_{12} = 3j_3$,$j_{13} = 3(j_5 + j_4) - j_2$,$j_{14} = j_6 + j_2(h_1 v_2)$;	(2M)

Tabelle 3.5: Falls $h_3, h_2, h_1 = 0$, ersetze $*_1, *_2, *_3$ und $*_4$ durch

$*_1$	$inv_1 = c_{10}^{-1}$,$c_{14} = inv_1$,$c_{15} = inv_1 c_9$,$c_{16} = 1$;	(M+I)
$*_2$	$d_{41} = -2h_0 t_3^2$,$d_{38} = 0$,$d_{39} = 0$,$d_{40} = 0$,$d_{42} = 0$,$d_{43} = 0$,$d_{44} = 0$;	(M+SQ)
$*_3$		
$*_4$	$j_{12} = 3j_3$,$j_{13} = 3(j_5 + j_4) - j_2$,$j_{14} = j_6$;	

Tabelle 3.6: Falls $h_3, h_2, h_1, h_0 = 0$, ersetze $*_1, *_2, *_3$ und $*_4$ durch

$*_1$	$inv_1 = c_{10}^{-1}$,$c_{14} = inv_1$,$c_{15} = inv_1 c_9$,$c_{16} = 1$;	(M+I)
$*_2$	$d_{38} = 0$,$d_{39} = 0$,$d_{40} = 0$,$d_{41} = 0$,$d_{42} = 0$,$d_{43} = 0$,$d_{44} = 0$;	
$*_3$		
$*_4$	$j_{12} = 3j_3$,$j_{13} = 3(j_5 + j_4) - j_2$,$j_{14} = j_6$;	

3.2.5 Die -2-adische Methode

Wir werden eine Methode zur Berechnung der Skalarmultiplikation

$$mg := \underbrace{g + \cdots + g}_{\text{m-mal}}$$

in Gruppen G, in denen die Berechnung von $-2g$ bzw. $-(g_1 + g_2)$ schneller als die von $2g$ bzw. $g_1 + g_2$ ist, beschreiben. Diese Methode eignet sich besonders für Jacobische nicht-hyperelliptischer Kurven vom Geschlecht 3, da in diesem Fall der beschriebene Algorithmus eine Beschleunigung von ca. 10% zur herkömmlichen *Double-and-Add* Methode nachweist. Für weitere Details siehe [4].

Zur Berechnung der Skalarmultiplikation mg in einer beliebigen Gruppe verwendet man standardmäßig die *Double-and-Add* Methode:

Algorithmus 4 Double-and-Add

INPUT: $m = \sum_{i=0}^{l(m)-1} m_i 2^i \in \mathbb{N}$, $m_i \in \{0, 1\}$, $g \in G$
OUTPUT: $e := mg$

1. Setze $e := g$
2. **for** $i = l(m) - 2$ to 0 **do**
  $e := 2e$
  if $m_i \neq 0$ **then**
    $e := e + g$
3. **return** e

Sei $w(m)$ die Anzahl der von 0 verschiedenen Bits m_i von m. Da die Dichte der von 0 verschiedenen Bits in der binären Entwicklung von m gleich $1/2$ ist, beträgt die Komplexität dieses Algorithmus $O(1 + \frac{1}{2}) \log_2(m)$ Gruppenoperationen.
Sei nun G eine Gruppe, in der die Berechnung von $-2g$ (bzw. $-(g_1+g_2)$) schneller als die Berechnung von $2g$ (bzw. $g_1 + g_2$) ist. Sei ferner $m = \sum_{i=0}^{l(m)-1} m_i 2^i$, $m_i \in \{0, \pm 1\}$ eine binäre Entwicklung von m. Möchte man in G die Skalarmultiplikation $7g$ berechnen, so wäre es günstiger $7g$ folgendermaßen zu berechnen:

$$7g := -(-2(-2(-2g)) + g).$$

Diese Idee lässt sich für die Berechnung vom mg, $m \in \mathbb{Z}$, verallgemeinern:

Algorithmus 5 -2-adische Entwicklung.

INPUT: $m = \sum_{i=0}^{l(m)-1} m_i 2^i \in \mathbb{N}$, $m_i \in \{0, \pm 1\}$, $g \in G$
OUTPUT: $e := mg$

1. Berechne und speichere $-g$

2. Berechne $l(m), w(m)$

3. Setze $e := (-1)^f g$, wobei $f := l(m) + w(m) \bmod 2$

4. **for** $i = l(m) - 2$ to 0 **do**
$e := -2e$
$f := 1 - f$
if $m_i \neq 0$ **then**
$e := -(e + (-1)^f m_i g)$
$f := 1 - f$

5. **return** e

Der Aufwand der Berechnung von $-2D$ bzw. $-(D_1 + D_2)$ für den speziellen Fall der Jacobischen einer nicht-hyperelliptischen Kurve

$$C : y^3 + h(x)y - f(x) = 0$$

vom Geschlecht 3 beträgt $130M + 12SQ + 2I$ bzw. $147M + 17SQ + 2I$: Schritt 3 des Algorithmus 3 wird für diese Berechnung nicht beachtet. Ebenso braucht man in Schritt 2.3 nur eine Inversion statt 2 Multiplikationen und eine Inversion um i_{20} zu berechnen, da die Berechnung von inv_2 nicht mehr notwendig ist.

Kapitel 4

Konstruktive Methode für den Satz von Torelli für g = 3

Unsere Hauptinteresse in diesem Kapitel besteht darin, den Satz von Torelli für eine 3-dimensionale über $\mathbb{C}$ definierte absolut einfache prinzipal polarisierte Abelsche Varietät A explizit und effizient zu lösen. Darunter versteht man folgendes: Finde die Gleichung einer Kurve C vom Geschlecht 3, so dass als prinzipal polarisierte Abelsche Varietäten gilt:

$$\mathrm{Jac}(C) \simeq A.$$

Nach dem Satz von Torelli ist die Kurve C bis auf Isomorphie eindeutig bestimmt. Das Entscheidungsproblem, ob die Kurve C hyperelliptisch ist oder nicht, wurde schon durch F. Oort mittels eines Kriteriums über das Verschwinden bestimmter gerader Thetanullwerte gelöst.

H-J. Weber [97] sowie auch J. Guàrdia [38] haben für das hyperelliptische Schottky-Problem effiziente Lösungen gegeben. Der nicht-hyperelliptische Fall, d.h. der generische Fall, wurde bis heute nicht genauer untersucht.

4.1 Abelsche Varietäten über $\mathbb{C}$

4.1.1 Polarisierung

Definition 4.1.1. Sei $\mathbb{C}^g/\Lambda$ ein komplexer Torus. Eine reellwertige alternierende Bilinearform $E(x, y)$ auf $\mathbb{C}^g$ heißt **Riemannform** auf $\mathbb{C}^g/\Lambda$, wenn

(i) $E(x, y) \in \mathbb{Z}$ für alle $x, y \in \Lambda$, und

(ii) $E(ix, y)$ eine positiv definite symmetrische Form ist.

Bemerkung 4.1.1. Falls H eine positiv definite Hermitesche Form auf $\mathbb{C}^g$ mit $\Im\mathrm{m}(H(\Lambda,\Lambda)) \subseteq \mathbb{Z}$ ist, so ist $\Im\mathrm{m}(H)$ eine Riemannform auf $\mathbb{C}^g/\Lambda$.

Jede über $\mathbb{C}$ definierte Abelsche Varietät ist zu einem Torus $\mathbb{C}^g/\Lambda$ isomorph. Ein komplexer Torus kommt genau dann von einer Abelschen Varietät, wenn es auf ihm eine Riemannform gibt. Das Paar $(\mathbb{C}^g/\Lambda, E)$ nennen wir dann **polarisierte Abelsche Varietät**.

Für jede polarisierte Abelsche Varietät $(\mathbb{C}^g/\Lambda, E)$ gibt es eine Basis $\{\lambda_1, \ldots, \lambda_{2g}\}$ von Λ, so dass die Matrixdarstellung von E bezüglich dieser Basis folgende Form

$$(E_{ij}) := (E(\lambda_i, \lambda_j))_{1\leq i,j\leq 2g} = \begin{pmatrix} 0 & \Delta \\ -\Delta & 0 \end{pmatrix}$$

mit einer Diagonalmatrix $\Delta \in M_{g,g}(\mathbb{Z})$ der Form

$$\Delta = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_g \end{pmatrix}, \quad e_i > 0, \quad e_1|e_2|\cdots|e_g$$

annimmt. In [80] ist ein Beweis dieser Aussage zu finden.

Eine Basis dieser Gestalt nennt man eine **symplektische Basis** für das Gitter Λ. Wir verweisen auf [53] für eine ausführliche Beschreibung eines Algorithmus zur Berechnung einer symplektischen Basis.

Das Gitter Λ lässt sich bezüglich einer symplektischen Basis $\{\lambda_1, \ldots, \lambda_{2g}\}$ in der Form

$$\Lambda = \Omega_1\mathbb{Z}^g + \Omega_2\mathbb{Z}^g$$

mit

$$\Omega_i = (\lambda_{1+(i-1)g}, \ldots, \lambda_{g+(i-1)g})$$

schreiben. Dabei erfüllen die Matrizen Ω_i die Riemann-Relationen

$$\Omega_2\Delta^{-1}\Omega_1^t = \Omega_1\Delta^{-1}\Omega_2^t, \quad 2i(\Omega_2\Delta^{-1}\overline{\Omega}_1^t - \Omega_1\Delta^{-1}\overline{\Omega}_2^t) > 0.$$

Aus den Riemann-Relationen ist leicht einzusehen, dass Ω_1 und Ω_2 invertierbar sind. Die Matrix

$$\Omega := \Delta\Omega_2^{-1}\Omega_1$$

nennen wir **Periodenmatrix** der Abelschen Varietät $(\mathbb{C}^g/\Lambda, E)$. Periodenmatrizen Abelscher Varietäten liegen in der **Siegelschen oberen Halbebene**

$$\mathbb{H}_g := \left\{\Omega \in \mathbb{C}^{g\times g} |\ \Omega^t = \Omega,\ \Im\mathrm{m}(\Omega) > 0\right\}.$$

Die **symplektische Gruppe**

$$\mathrm{Sp}(2g,\mathbb{Z}) := \left\{\gamma = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{GL}(2g,\mathbb{Z}) |\ \gamma^t J \gamma = J \text{ mit } J := \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix}\right\}$$

operiert via

$$\gamma(z,\Omega) := ((C\Omega + D)^{-1}z, (A\Omega + B)(C\Omega + D)^{-1})$$

auf $\mathbb{C}^g \times \mathbb{H}_g$.

Die Abelsche Varietät $(\mathbb{C}^g/\Lambda, E)$ heißt **prinzipal polarisiert**, falls eine symplektische Basis $\{\lambda_1, \ldots, \lambda_{2g}\}$ existiert, so dass

$$(E_{ij}) := (E(\lambda_i, \lambda_j))_{1\le i,j\le 2g} = \begin{pmatrix} 0 & E_g \\ -E_g & 0 \end{pmatrix}$$

gilt. In diesem Fall ist das Gitter zu $L_\Omega := \mathbb{Z}^g + \Omega\mathbb{Z}^g$ äquivalent. Die Nebenklasse $\mathrm{Sp}(2g,\mathbb{Z})\Omega$ entspricht in diesem Fall genau der Isomorphieklasse der prinzipal polarisierten Abelschen Varietät $(\mathbb{C}^g/\Lambda, E)$ in $\mathrm{Sp}(2g,\mathbb{Z}) \setminus \mathbb{H}_g$.

Nicht jede Abelsche Varietät über $\mathbb{C}$ ist prinzipal polarisiert, aber:

Proposition 4.1.1. ([13, p. 75 - VI.6.3]) Jede Abelsche Varietät über $\mathbb{C}$ ist isogen zu einer prinzipal polarisierten Abelschen Varietät.

Für den Begriff der prinzipalen Polarisierung gibt es auch eine äquivalente, algebraische Definition für beliebige Definitionskörper k (siehe [63]).

Eine meromorphe Funktion ϑ auf $\mathbb{C}^g$ heißt **Thetafunktion** auf $\mathbb{C}^g/\Lambda$, wenn

$$\vartheta(z+\lambda) = \vartheta(z) \cdot \exp\left(2\pi i(l_\lambda(z) + c_\lambda)\right) \quad \text{für alle } \lambda \in \Lambda,$$

für geeignete $\mathbb{C}$-Linearformen $l_\lambda(z)$ auf $\mathbb{C}^g$, und von λ abhängige komplexe Zahlen c_λ. Dies erzwingt

$$l_{\lambda_1+\lambda_2}(z) = l_{\lambda_1}(z) + l_{\lambda_2}(z),$$

und daher kann man $l_{\lambda_1}(z)$ zu einer $\mathbb{R}$-bilinearen Funktion auf $\mathbb{C}^g$ fortsetzen. Ist ϑ holomorph, so wird durch

$$E_\vartheta(x,y) := l_x(y) - l_y(x)$$

wegen

$$l_{\lambda_1}(\lambda_2) \equiv l_{\lambda_2}(\lambda_1) \mod \mathbb{Z}$$

eine Riemannform E_ϑ auf $\mathbb{C}^g/\Lambda$ definiert.

Ist anderseits $E(x,y)$ eine Riemannform auf $\mathbb{C}^g/\Lambda$, so gibt es eine holomorphe Thetafunktion θ auf $\mathbb{C}^g/\Lambda$, so dass $E = E_\theta$ ist, nämlich die **Riemannsche Thetafunktion**

$$\theta(z,\Omega) := \sum_{n\in\mathbb{Z}^g} \exp(\pi i(n\Omega n^t + 2nz)),$$

welche auf $\mathbb{C}^g \times \mathbb{H}_g$ holomorph ist. Die Positivdefinitheit des Imaginärsteils von Ω sichert die absolute und auf jeder kompakten Teilmenge von $\mathbb{C}^g \times \mathbb{H}_g$ gleichmäßige Konvergenz der Reihe.

Eine der wichtigsten Eigenschaften der Riemannschen Thetafunktion ist ihre „quasi-Periodizität“ bezüglich $z \longmapsto z + a$ für alle $a \in L_\Omega$. Dabei heißt θ quasi-periodisch, falls θ periodisch bis auf einen einfachen multiplikativen Faktor ist. Genauer gesagt, wenn gilt:

$$\theta(z+m,\Omega) = \theta(z,\Omega) \text{ und } \theta(z+\Omega m,\Omega) = \exp(-\pi i(m\Omega m^t + 2mz)) \cdot \theta(z,\Omega)$$

für alle $z \in \mathbb{C}^g$ und $m \in \mathbb{Z}^g$.

Für die Menge der 2-Torsionspunkte $A[2]$ von $A = \mathbb{C}^g/\Lambda$, also für den Kern der Isogenie

$$[2] : A \longrightarrow A, \quad a \longmapsto 2a$$

gilt

$$A[2] = \left\{ z_m = \frac{1}{2}\Omega\delta^t + \frac{1}{2}\,\epsilon^t \;\middle|\; m = \begin{bmatrix}\delta\\ \epsilon\end{bmatrix} \text{ mit } \delta,\epsilon \in \mathbb{Z}^g \bmod 2\mathbb{Z}^g \right\}.$$

Der Torsionspunkt z_m heißt **gerade** (bzw. **ungerade**) falls $\delta\epsilon^t \equiv 0 \mod 2$ (bzw. $\delta\epsilon^t \equiv 1 \mod 2$). Die Menge $A[2]$ der 2-Torsionspunkte zerfällt in zwei disjunkte Mengen $\sum^+$ und $\sum^-$ von geraden und ungeraden 2-Torsionspunkten.

4.1.2 Jacobische Varietäten

Jacobische Varietäten von Kurven lassen sich prinzipal polarisieren (siehe [64] für beliebige Körper):

Eine über $\mathbb{C}$ definierte Kurve C vom Geschlecht g ist eine kompakte Riemannsche Fläche mit g Henkeln. Ihre erste **Homologiegruppe** $H_1(C,\mathbb{Z})$ ist eine freie

Abelsche Gruppe mit $2g$ Erzeugern. Als Basis von $H_1(C, \mathbb{Z})$ wählen wir geschlossene Kurven $a_1, \ldots, a_g, b_1, \ldots, b_g$ auf C derart, dass sich die Kurven a_i und a_j, b_i und b_j, a_i und b_j für $i \neq j$ in keinem Punkt, aber die Kurven a_i und b_i sich in genau einem Punkt schneiden.

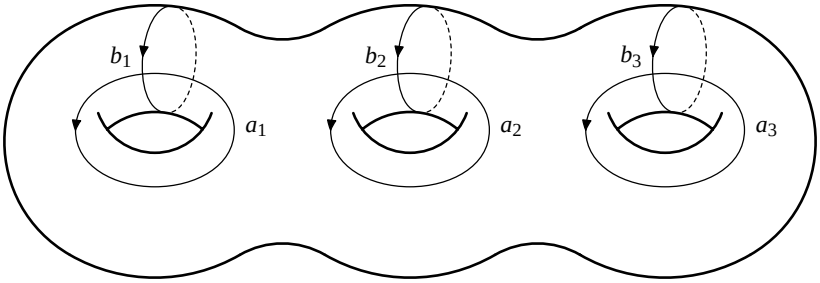


Abbildung 4.1: Homologiegruppe auf einer Riemannschen Fläche, $g = 3$

Es gibt eine Basis $\{w_1, \ldots, w_g\}$ des Vektorraumes der holomorphen Differentialformen $\Omega^1(C)$ von C mit

$$\int_{a_i} w_j = \delta_{ij}.$$

Definiert man anschließend

$$\Omega_{ij} := \int_{b_i} w_j \quad \text{und} \quad \Omega := (\Omega_{ij})_{1 \leq i,j \leq g},$$

so liegt Ω in $\mathbb{H}_g$. Nach dem Satz von **Abel** ist die Gruppe $\mathrm{Jac}(C)(\mathbb{C})$ der komplexen Punkte der Jacobischen Varietät $\mathrm{Jac}(C)$ komplex analytisch isomorph zum Torus $\mathbb{C}^g / L_\Omega$ mit dem Gitter $L_\Omega = \mathbb{Z}^g + \Omega\mathbb{Z}^g$.

Die **Abel-Jacobi** Abbildung Φ definiert durch

$$\begin{array}{rccl} \Phi: & \mathrm{Jac}(C)(\mathbb{C}) & \longrightarrow & \mathbb{C}^g / L_\Omega \\ & (\sum_{i=1}^r P_i - rP_\infty) & \longmapsto & \sum_{i=1}^r \int_{P_\infty}^{P_i} (w_1, \ldots, w_g) \mod L_\Omega \end{array}$$

liefert den Isomorphismus.

Im folgenden identifizieren wir das d-fache symmetrische Produkt C_d von C mit der Menge der effektiven Divisoren vom Grad d von C.

Definition 4.1.2. Der **Theta Divisor** Θ von $\mathrm{Jac}(C)$ ist definiert als die *Nullstellenmenge* der Riemannschen Thetafunktion $\theta(z, \Omega)$.

Das Bild von C_{g-1} unter der Abel-Jacobi-Abbildung ist bis auf Translation um ein Element $\kappa \in \mathrm{Jac}(C)$ gleich dem Theta Divisor Θ. Wir bezeichnen κ als die **Riemannsche Konstante**. Genauer gilt:

Satz 4.1.1 (**Riemann**, [69])**.** Für die Riemannsche Thetafunktion $\theta(z, \Omega)$ gilt:

$$\theta(z, \Omega) = 0 \Longleftrightarrow z = \Phi(Q_1 + \cdots + Q_{g-1}) - \kappa \text{ mit } Q_i \in C.$$

Dabei ist die Riemannsche Konstante κ durch den Basispunkt P_∞ der Abel-Jacobi-Abbildung eindeutig bestimmt, und es gilt $\kappa = \Phi(D_0)$ für einen halbkanonischen Divisor D_0 von C, d.h. ein Divisor mit $2D_0 \sim K_C$.

Die durch

$$\begin{array}{rccc} \Pi: & C_{g-1} & \longrightarrow & \mathbb{C}^g/L_\Omega \\ & D := \sum_{i=1}^{g-1} P_i & \longmapsto & \Phi(D) + \kappa \end{array}$$

definierte Abbildung Π erfüllt die Symmetrie-Eigenschaft

$$\Pi(K_C - D) = -\Pi(D) \text{ für alle } D \in C_{g-1},$$

dabei ist K_C ein kanonischer Divisor von C.
Die kanonische Abbildung ϕ von C hat bezüglich der Basis der holomorphen Differentiale $\{\omega_1, \ldots, \omega_g\}$ von C folgende Darstellung

$$\begin{array}{rccc} \phi: & C & \longrightarrow & \mathbb{P}^{g-1} \\ & P & \longmapsto & \phi(P) := (\omega_1(P) : \cdots : \omega_g(P)). \end{array}$$

Proposition 4.1.2 ([37])**.** Sei C eine über einem Zahlkörper K definierte Kurve vom Geschlecht g. Seien $P_1, \ldots, P_{g-1} \in C(\bar{K})$, so dass für den Divisor $D := P_1 + \cdots + P_{g-1}$ gilt $l(D) = 1$. Dann beschreibt die Gleichung

$$H_D(X_1, \ldots, X_g) := \left(\frac{\partial \theta}{\partial z_1}(\Pi(D)), \ldots, \frac{\partial \theta}{\partial z_g}(\Pi(D)) \right) \Omega_1^{-1} \begin{pmatrix} X_1 \\ \vdots \\ X_g \end{pmatrix} = 0$$

eine Hyperebene von $\mathbb{P}^{g-1}$ durch den Divisor $\phi(D)$ (in $\phi(C)$).

4.1.3 Schottky-Problem

Ein Isomorphismus zwischen zwei prinzipal polarisierten Abelschen Varietäten (A_1, E_1) und (A_2, E_2) ist ein Isomorphismus zwischen den Varietäten A_1 und A_2, der die prinzipal Polarisierungen E_1 und E_2 ineinander überführt. Ein Isomorphismus von Kurven induziert (bis auf Translation) einen Isomorphismus prinzipal polarisierter Jacobischer Varietäten. Nach dem Satz von **Torelli** gilt auch die Umkehrung:

Satz 4.1.2 (**Torelli** [98])**.** Sind die Jacobischen Varietäten (Jac_1, E_1) und (Jac_2, E_2) zweier Kurven C_1 und C_2 vom Geschlecht g als prinzipal polarisierte Abelsche Varietäten isomorph, so sind die Kurven C_1 und C_2 isomorph.

Bemerkung 4.1.2. Der Satz von Torelli besagt genau, dass eine Kurve durch ihre Jacobische und die darauf definierte Polarisierung eindeutig bestimmt ist. Betrachtet man sie aber als „unpolarisierte“ Abelsche Varietäten, so besteht die Möglichkeit, dass zwei nicht-isomorphe Kurven isomorphe Jacobische besitzen ([46, 56, 31]). In [44] gibt Howe zu $n \in \mathbb{N}$ eine explizite Methode an, um n paarweise nicht-isomorphe glatte ebene Quartiken und eine hyperelliptische Kurve vom Geschlecht 3 zu konstruieren, die als unpolarisierte Abelsche Varietäten die gleiche nicht-einfache Jacobische haben. Im generischen Fall besitzt aber eine prinzipal polarisierbare Abelsche Varietät genau eine Isomorphieklasse von prinzipalen Polarisierungen.

Unser Ziel ist eine explizite *Konstruktion* des Satzes von Torelli. Darunter verstehen wir die folgende Aufgabe:
Finde zu einer vorgegebenen prinzipal polarisierten Abelschen Varietät A, die die Jacobische einer Kurve definiert, die Gleichung einer Kurve C (bis auf Isomorphie) mit $\mathrm{Jac}(C) \simeq A$.

Sei weiterhin $k = \mathbb{C}$ und $\mathcal{A}_g(k)$ der grobe Modulraum der k-Isomorphieklassen prinzipal polarisierter Abelscher Varietäten der Dimension g. Dieser grobe Modulraum ist nach der Arbeit von Mumford [68] als Varietät irreduzibel und besitzt die Dimension $g(g+1)/2$. Sei ferner $\mathcal{M}_g(k)$ der grobe Modulraum der Dimension $3(g-1)$ bestehend aus den k-Isomorphieklassen von Kurven vom Geschlecht g (siehe [16]). Seine Untervarietät $\mathcal{H}_g(k)$, die aus den k-Isomorphieklassen von hyperelliptischen Kurven vom Geschlecht g besteht, hat die Dimension $2g-1$.

Mittels der Abel-Jacobi-Abbildung Jac bettet man $\mathcal{M}_g(k)$ sowie auch $\mathcal{H}_g(k)$ als grobe Modulräume in $\mathcal{A}_g(k)$ ein. Dann gilt

$$\mathrm{codim}_{\mathcal{A}_g(k)}\mathrm{Jac}(\mathcal{M}_g(k)) = \frac{1}{2}(g-2)(g-3),$$

$$\mathrm{codim}_{\mathcal{A}_g(k)}\mathrm{Jac}(\mathcal{H}_g(k)) = \frac{1}{2}(g-1)(g-2).$$

Dies bedeutet für $g = 3$, dass alle prinzipal polarisierten Abelschen Varietäten Jacobische von Kurven sind, aber im allgemeinen nicht mehr Jacobische von hyperelliptischen Kurven.

Das **Schottky-Problem** fragt nach der Charakterisierung des Jacobi-Ortes $\mathrm{Jac}(\mathcal{M}_g(k))$ in $\mathcal{A}_g(k)$. Dazu gelang C. Poor [73] eine genaue Charakterisierung für den hyperelliptischen Jacobi-Ort anzugeben, die aus dem Verschwinden einer Anzahl von Thetanullwerte besteht.

4.1.4 Riemannsche Thetafunktion und Thetanullwerte

Sei A eine prinzipal polarisierte Abelsche Varietät der Dimension g und Periodenmatrix $\Omega \in \mathbb{H}_g$. Zwei Zeilenvektoren $\delta, \epsilon \in \mathbb{Z}^g \bmod 2\mathbb{Z}^g$, den **Charakteristiken**, ordnen wir die auf $\mathbb{C}^g \times \mathbb{H}_g$ holomorphe Thetafunktion mit Periodenmatrix Ω,

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} : \mathbb{C}^g \times \mathbb{H}_g \longrightarrow \mathbb{C}$$

definiert durch

$$\begin{aligned} \theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (z, \Omega) &:= \sum_{n \in \mathbb{Z}^g} \exp\left(\pi i \left((n + \frac{1}{2}\delta)\Omega(n + \frac{1}{2}\delta)^t + 2(n + \frac{1}{2}\delta)(z + \frac{1}{2}\epsilon^t)\right)\right) \\ &= \exp\left(\frac{\pi i}{4}\delta\Omega\delta^t + \pi i\delta(z + \frac{\epsilon^t}{2})\right) \cdot \theta\left(z + \frac{1}{2}\Omega\delta^t + \frac{\epsilon^t}{2}, \Omega\right) \end{aligned}$$

zu. Die Abbildung

$$(\mathbb{Z}^g \bmod 2\mathbb{Z}^g)^2 \longrightarrow A[2],\ m = \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} \longmapsto z_m := \frac{1}{2}\Omega\delta^t + \frac{\epsilon^t}{2}$$

bildet eine Bijektion zwischen den Charakteristiken und den 2-Torsionspunkten von A.

Die Funktionen

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (0, \Omega) : \mathbb{H}_g \longrightarrow \mathbb{C}$$

heißen **Thetanullwerte**. $\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (0, \Omega)$ heißt **gerade**, falls $\delta\epsilon^t \equiv 0 \pmod 2$ sonst **ungerade**, und wegen

$$\theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (-z, \Omega) = (-1)^{\delta\epsilon^t} \theta \begin{bmatrix} \delta \\ \epsilon \end{bmatrix} (z, \Omega)$$

verschwinden die ungeraden Thetanullwerten identisch. Es gibt $2^{g-1}(2^g + 1)$ gerade und $2^{g-1}(2^g - 1)$ ungerade Thetanullwerte. Das Verschwinden der geraden Thetanullwerte ist invariant unter der Operation der symplektischen Gruppe, denn

Proposition 4.1.3. ([48, V.2])
Sei $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in \mathrm{Sp}(2g, \mathbb{Z})$. Sei $A_0 = \mathrm{diag}(A)$ und

$$\phi_{[\delta,\varepsilon]}(M) = -\delta D B \delta^t + 2\delta B C \epsilon^t - \epsilon C A \epsilon^t + (D\epsilon^t - C\delta^t) \cdot (A^t B)_0.$$

Dann gilt

$$\theta \begin{bmatrix} 2(D\delta^t - C\epsilon^t) + (C^t D)_0 \\ 2(-B\delta^t + A\epsilon^t) + (A^t B)_0 \end{bmatrix} \left(0, (A\Omega + B)(C\Omega + D)^{-1}\right) =$$
$$\kappa(M) \cdot \exp\left(\pi i \phi_{[\delta,\varepsilon]}(M)\right) \cdot \det(C\Omega + D)^{1/2} \cdot \theta \begin{bmatrix} 2\delta \\ 2\epsilon \end{bmatrix} (0, \Omega),$$

wobei $\kappa(M)^2$ eine Einheitswurzel ist, die nur von M abhängig ist.

In [99] hat A. Weng einen Algorithmus zur effizienten Berechnung von Thetanullwerten angegeben.

Bemerkung 4.1.3. Möchte man die Thetanullwerte noch effizienter berechnen, so wäre es sinnvoll erst die Periodenmatrix Ω im Siegelschen Fundamentalbereich zu reduzieren, und dann die Thetanullwerte zu bestimmen. In diesem Fall konvergieren sie schneller. Allerdings gibt es für $g \geq 3$ bis heute keinen Algorithmus zur Siegel-Reduktion (siehe [36] für $g = 2$).

4.2 Konstruktive Methode für den Satz von Torelli für $\mathbf{g = 3}$

Sei im folgenden $A = \mathbb{C}^3/(\Omega_1\mathbb{Z}^3 + \Omega_2\mathbb{Z}^3)$ eine prinzipal polarisierte Abelsche Varietät mit Periodenmatrix $\Omega := \Omega_2^{-1}\Omega_1 \in \mathbb{H}_3$. Dann gilt:

Satz 4.2.1. Sei Ω eine beliebige Periodenmatrix einer absolut einfachen prinzipal polarisierten Abelschen Varietät der Dimension 3.

(i) Ω ist hyperelliptisch genau dann, wenn genau ein gerader Thetanullwert in Ω verschwindet.

(ii) Ω ist nicht-hyperelliptisch genau dann, wenn keiner ihrer geraden Thetanullwerte verschwindet.

Gilt $\mathrm{char}(k) \neq 2$, und ist C/k eine nicht-hyperelliptische Kurve vom Geschlecht 3, so hat C wegen Proposition 3.1.2 genau 28 Bitangenten. Die Menge der 28 Bitangenten steht in Bijektion mit der Menge der ungeraden 2-Torsionspunkte

von Jac(C) (siehe [78]), und wegen Proposition 4.1.2 ist die dem ungeraden 2-Torsionspunkt z_0 entsprechende Bitangente gegeben durch die Gerade mit der Gleichung

$$\left(\frac{\partial\theta}{\partial z_1}(z_0), \frac{\partial\theta}{\partial z_2}(z_0), \frac{\partial\theta}{\partial z_3}(z_0)\right) \Omega_1^{-1} \begin{pmatrix} Z \\ X \\ Y \end{pmatrix} = 0. \tag{4.1}$$

Definition 4.2.1. Sei $S = ([\epsilon_i])_{i=1,\dots,7}$ eine Menge von Charakteristiken. Die Menge S heißt **Fundamentalsystem** falls gilt:

(i) Jede ungerade Charakteristik kann durch $[\epsilon_i]$ oder $[\epsilon_i]+[\epsilon_j]$, $i \neq j$, beschrieben werden, und

(ii) Jede gerade Charakteristik kann durch $[0]$ oder $[\epsilon_i] + [\epsilon_j] + [\epsilon_k]$, mit paarweisen verschiedenen i, j, k beschrieben werden.

Die Menge $S := ([\epsilon_i])_{i=1,\dots,7}$ mit

$$\epsilon_1 = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \epsilon_2 = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix} \quad \epsilon_3 = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} \quad \epsilon_4 = \begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$
$$\epsilon_5 = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix} \quad \epsilon_6 = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix} \quad \epsilon_7 = \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix},$$

bildet ein Fundamentalsystem. Seien nun β_i (bzw. β_{ij}) die zu $[\epsilon_i]$ (bzw. $[\epsilon_i]+[\epsilon_j]$) assoziierten Bitangenten. Die Menge (β_i) bildet ein **Aronhold-System**, also eine Menge von Bitangenten mit der Eigenschaft, dass die Schnittpunkte (mit der Quartik) von drei beliebigen Bitangenten dieser Menge nie auf einer Quadrik liegen (siehe [19])).
Nach linearen Transformationen können wir o.B.d.A. annehmen, dass

$$\begin{cases} \beta_1 : x_1 = 0 & \beta_5 : a_1x_1 + a_2x_2 + a_3x_3 = 0 \\ \beta_2 : x_2 = 0 & \beta_6 : a_1'x_1 + a_2'x_2 + a_3'x_3 = 0 \\ \beta_3 : x_3 = 0 & \beta_7 : a_1''x_1 + a_2''x_2 + a_3''x_3 = 0 \\ \beta_4 : x_1 + x_2 + x_3 = 0 & \end{cases} \tag{4.2}$$

Die umgekehrte Frage, ob die obigen $(\beta_i)_{i=1,\dots,7}$ als Aronhold-System einer glatten Quartik C auftreten können, wurde schon in 1898 durch Riemann [77] gelöst. Ferner gab Riemann auch eine Methode an, wie man aus der Menge $(\beta_i)_{i=1,\dots,7}$ eine glatte Quartik berechnet, die die $(\beta_i)_{i=1,\dots,7}$ als Aronhold-System besitzt. Erst vor kurzem haben L. Caporaso, E. Sernesi [11] und D. Lehavi [59] bewiesen, dass eine solche Quartik durch $(\beta_i)_{i=1,\dots,7}$ (bis auf Isomorphie) eindeutig bestimmt ist.

Satz 4.2.2 (**Riemann**, [77])**.**
Die Quartik C ist isomorph zur Quartik, die wir als **Riemann-Modell** bezeichnen, mit der Gleichung

$$\sqrt{x_1 v_1} + \sqrt{x_2 v_2} + \sqrt{x_3 v_3} = 0, \tag{4.3}$$

dabei sind v_1, v_2, v_3 gegeben durch

$$\begin{cases} v_1 + v_2 + v_3 + x_1 + x_2 + x_3 = 0 \\ \frac{v_1}{a_1} + \frac{v_2}{a_2} + \frac{v_3}{a_3} + ka_1x_1 + ka_2x_2 + ka_3x_3 = 0 \\ \frac{v_1}{a_1'} + \frac{v_2}{a_2'} + \frac{v_3}{a_3'} + k'a_1'x_1 + k'a_2'x_2 + k'a_3'x_3 = 0 \\ \frac{v_1}{a_1''} + \frac{v_2}{a_2''} + \frac{v_3}{a_3''} + k''a_1''x_1 + k''a_2''x_2 + k''a_3''x_3 = 0 \end{cases}$$

und k, k', k'' Lösungen der Gleichungen

$$\begin{pmatrix} \frac{1}{a_1} & \frac{1}{a_1'} & \frac{1}{a_1''} \\ \frac{1}{a_2} & \frac{1}{a_2'} & \frac{1}{a_2''} \\ \frac{1}{a_3} & \frac{1}{a_3'} & \frac{1}{a_3''} \end{pmatrix} \begin{pmatrix} \lambda \\ \lambda' \\ \lambda'' \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix},$$

$$\begin{pmatrix} a_1 & a_1' & a_1'' \\ a_2 & a_2' & a_2'' \\ a_3 & a_3' & a_3'' \end{pmatrix} \begin{pmatrix} \lambda k \\ \lambda' k' \\ \lambda'' k'' \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}.$$

Ferner gelten für die 28 Bitangenten

$$\beta_1 : x_1 = 0 \quad \beta_2 : x_2 = 0 \quad \beta_3 : x_3 = 0$$
$$\beta_{23} : v_1 = 0 \quad \beta_{13} : v_2 = 0 \quad \beta_{12} : v_3 = 0$$

$$\beta_4 : x_1 + x_2 + x_3 = 0 \qquad \beta_5 : a_1x_1 + a_2x_2 + a_3x_3 = 0$$
$$\beta_6 : a_1'x_1 + a_2'x_2 + a_3'x_3 = 0 \quad \beta_7 : a_1''x_1 + a_2''x_2 + a_3''x_3 = 0$$

$$\beta_{14} : v_1 + x_2 + x_3 = 0 \qquad \beta_{15} : \tfrac{v_1}{a_1} + ka_2x_2 + ka_3x_3 = 0$$
$$\beta_{16} : \tfrac{v_1}{a_1'} + k'a_2'x_2 + k'a_3'x_3 = 0 \quad \beta_{17} : \tfrac{v_1}{a_1''} + k''a_2''x_2 + k''a_3''x_3 = 0$$

$$\beta_{24} : x_1 + v_2 + x_3 = 0 \qquad \beta_{25} : ka_1x_1 + \tfrac{v_2}{a_2} + ka_3x_3 = 0$$
$$\beta_{26} : k'a_1'x_1 + \tfrac{v_2}{a_2'} + k'a_3'x_3 = 0 \quad \beta_{27} : k''a_1''x_1 + \tfrac{v_2}{a_2''} + k''a_3''x_3 = 0$$

$$\beta_{34} : x_1 + x_2 + v_3 = 0 \qquad \beta_{35} : ka_1x_1 + ka_2x_2 + \tfrac{v_3}{a_3} = 0$$
$$\beta_{36} : k'a_1'x_1 + k'a_2'x_2 + \tfrac{v_3}{a_3'} = 0 \quad \beta_{37} : k''a_1''x_1 + k''a_2''x_2 + \tfrac{v_3}{a_3''} = 0$$

$$\beta_{67} : \tfrac{v_1}{1-ka_2a_3} + \tfrac{v_2}{1-ka_3a_1} + \tfrac{v_3}{1-ka_1a_2} = 0$$
$$\beta_{57} : \tfrac{v_1}{1-k'a_2'a_3'} + \tfrac{v_2}{1-k'a_3'a_1'} + \tfrac{v_3}{1-k'a_1'a_2'} = 0$$
$$\beta_{56} : \tfrac{v_1}{1-k''a_2''a_3''} + \tfrac{v_2}{1-k''a_3''a_1''} + \tfrac{v_3}{1-k''a_1''a_2''} = 0$$

$$\beta_{45} : \tfrac{v_1}{a_1(1-ka_2a_3)} + \tfrac{v_2}{a_2(1-ka_3a_1)} + \tfrac{v_3}{a_3(1-ka_1a_2)} = 0$$
$$\beta_{46} : \tfrac{v_1}{a_1'(1-k'a_2'a_3')} + \tfrac{v_2}{a_2'(1-k'a_3'a_1')} + \tfrac{v_3}{a_3'(1-k'a_1'a_2')} = 0$$
$$\beta_{47} : \tfrac{v_1}{a_1''(1-ka_2''a_3'')} + \tfrac{v_2}{a_2''(1-k''a_3''a_1'')} + \tfrac{v_3}{a_3''(1-k''a_1''a_2'')} = 0$$

Ist nun eine (absolut einfache) prinzipal polarisierte Abelsche Varietät der Dimension 3 durch ihre Torusdarstellung $A = \mathbb{C}^3/(\Omega_1\mathbb{Z}^3 + \Omega_2\mathbb{Z}^3)$ (mit $\Omega_1^{-1}\Omega_2 \in \mathbb{H}_3$) gegeben, so geht man folgendermaßen vor, um die Gleichung einer Kurve $C/\mathbb{C}$ mit $\mathrm{Jac}(C) \simeq_{\mathbb{C}} A$ zu finden:

(i) Durch die Berechnung der 36 geraden Thetanullwerte von A entscheidet man gemäß Satz 4.2.1, ob $A \notin \mathrm{Jac}(\mathcal{H}_3(\mathbb{C}))$.

(ii) Ist $A \notin \mathrm{Jac}(\mathcal{H}_3(\mathbb{C}))$, so berechnet man in effizienter Weise die Ableitungen der Thetafunktionen an den ungeraden 2-Torsionspunkten $z_{\epsilon_i}(\epsilon_i \in S)$ und somit mittels (4.1) auch die Gleichungen der 7 Bitangenten β_i des Aronhold-Systems S.

(iii) Nach linearen Transformationen erreicht man leicht, dass die vier zu den Charakteristiken $[\epsilon_i]_{i=1\ldots,4}$ assoziierten Bitangenten β_i die kanonische Form (4.2) annehmen. Mittels Satz 4.2.2 berechnet man die Gleichung der Quartik im Riemann-Modell $C/\mathbb{C}$ mit $\mathrm{Jac}(C) \simeq_{\mathbb{C}} A$.

Kapitel 5

Modulare Kurven und modulare Jacobische der Dimension 3

Wir werden uns im folgenden mit heute besonders gut verstandenen Abelschen Varietäten über $\mathbb{Q}$ beschäftigen, die die Eigenschaft haben, dass an Primidealen $\mathfrak{p}$ mit guter Reduktion die Anzahl der Punkte $\#A(k_\mathfrak{p})$ effizient berechenbar ist. Wir werden uns hauptsächlich mit $\mathbb{Q}$-einfachen Faktoren der Jacobischen von Modulkurven $X_0(N)$ beschäftigen.

5.1 Modulkurven $X_0(N)$

5.1.1 Grundlegende Definitionen

Sei $\mathrm{SL}_2(\mathbb{Z})$ die Gruppe der ganzzahligen Matrizen mit Determinante 1. Zu der natürlichen Zahl N sei

$$\Gamma_0(N) := \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) |\ c \equiv 0 \mod N \right\}$$

die **Hecke**-Untergruppe der Stufe N von $\mathrm{SL}_2(\mathbb{Z})$. Bezeichnen wir mit

$$\mathbb{H} := \{\tau \in \mathbb{C} |\ \Im\mathrm{m}(\tau) > 0\}$$

die komplexe obere Halbebene und mit

$$\mathbb{H}^* := \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$$

die erweiterte komplexe obere Halbebene unter Hinzunahme der **Spitzen** $\mathbb{Q}$ und ∞, so operiert $\mathrm{SL}_2(\mathbb{Z})$ sowie $\Gamma_0(N)$ auf $\mathbb{H}^*$ vermöge der gebrochenen linearen Transformationen

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} z \longmapsto \frac{az+b}{cz+d}.$$

Die Bahnen dieser Operation unter $\Gamma_0(N)$ bezeichnen wir mit

$$Y_0(N) := \Gamma_0(N) \setminus \mathbb{H} \subset \Gamma_0(N) \setminus \mathbb{H}^* =: X_0(N).$$

$X_0(N)$ ist eine kompakte Riemannsche Fläche und damit eine über $\mathbb{C}$ definierte projektive algebraische Kurve, die wir im folgenden als die **Modulkurve von** $\Gamma_0(N)$ bezeichnen. Sei g das Geschlecht von $X_0(N)$. Als kompakte Riemannsche Fläche mit g Henkeln hat die erste Homologiegruppe $H_1(X_0(N), \mathbb{Z})$ von $X_0(N)$ den Rang $2g$.

Sei

$$\epsilon : (\mathbb{Z}/N\mathbb{Z})^* \longrightarrow \mathbb{C}^*$$

ein **Dirichlet-Charakter** mit Führer $\mathrm{cond}(\epsilon)|N$.

Definition 5.1.1. Eine holomorphe Funktion $f : \mathbb{H} \longrightarrow \mathbb{C}$ heißt **Modulform** (bzw. **Spitzenform**) vom Gewicht k, Charakter (Nebentyp) ϵ und Stufe N bezüglich $\Gamma_0(N)$, falls f die folgenden Bedingungen erfüllt:

(i) $f(\gamma\tau) = \epsilon(d)(c\tau + d)^k f(\tau)$ für alle $\tau \in \mathbb{H}$, $\gamma \in \Gamma_0(N)$ mit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$

(ii) f ist holomorph in den Spitzen von $\Gamma_0(N)$ fortsetzbar (und vesrschwindet dort).

Der $\mathbb{C}$-Vektorraum der Modul- bzw. Spitzenformen vom Gewicht k, Charakter ϵ und Stufe N wird mit $M_k(N, \epsilon)$ bzw. $S_k(N, \epsilon)$ bezeichnet. Ist der Charakter ϵ trivial, so bezeichnet man diese Vektorräume kurz mit $M_k(N)$ bzw. $S_k(N)$.

Lemma 5.1.1. Die Abbildung ω definiert durch

$$\omega : S_2(N) \longrightarrow \Omega^1(X_0(N)), \;\; f(\tau) \longmapsto 2\pi i f(\tau) d\tau$$

induziert einen Isomorphismus zwischen dem Vektorraum der Spitzenformen $S_2(N)$ und dem Vektorraum der holomorphen Differentialformen $\Omega^1(X_0(N))$ von $X_0(N)$. Die Dimension von $S_2(N)$ als $\mathbb{C}$-Vektorraum ist gleich dem Geschlecht der Modulkurve $X_0(N)$.

Modulformen (zu $\Gamma_0(N)$) sind periodisch, denn aus $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N)$ folgt $f(\tau + 1) = f(\tau)$. Somit besitzen Modulformen in der Spitze ∞ eine Fourier-Entwicklung der Gestalt

$$f(\tau) = \sum_{n=0}^{\infty} a_n q^n \quad , \qquad \text{wobei } q = e^{2\pi i \tau} \text{ und } a_n \in \mathbb{C}.$$

Spitzenformen haben eine Fourier-Entwicklung

$$f(\tau) = \sum_{n=1}^{\infty} a_n q^n \quad , \quad q = e^{2\pi i \tau}.$$

Modulformen lassen sich durch ihre Fourier-Koeffizienten unterscheiden. Man hat das folgende effektive Kriterium:

Satz 5.1.1 ([81])**.** Sei $\mu := [\mathrm{SL}_2(\mathbb{Z}) : \Gamma_0(N)] = N \prod_{p|N}(1 + p^{-1})$ und $f(\tau) = \sum_{n=0}^{\infty} a_n q^n$ mit $q = e^{2\pi i \tau}$ eine Modulform vom Gewicht k und Stufe N. Sind alle Koeffizienten a_n für $0 \leq n \leq \mu k/12$ gleich 0, dann ist $f(\tau)$ identisch 0.

5.1.2 Hecke-Operatoren

Hier werden wir uns hauptsächlich mit der Operation von **Hecke-Operatoren** auf Modulformen $f(\tau) \in M_k(N)$, sowie auf die Jacobische $J_0(N)$ von $X_0(N)$ beschäftigen. Wir verzichten auf eine genaue Definition der Hecke-Algebra und verweisen auf das Buch von Shimura [84].

Lemma 5.1.2. Sei $f(\tau) = \sum_{n=0}^{\infty} a_n q^n \in M_k(N)$ und p eine Primzahl. Dann ist

$$b_n := a_{pn} + p^{k-1} \cdot a_{n/p}$$

der n-te Fourier-Koeffizient von $T_p(f(\tau)) = \sum_{n=0}^{\infty} b_n q^n$, wobei $a_{n/p} = 0$ für $p \nmid n$. Ferner gilt:

$$T_{p^n} = \begin{cases} T_p T_{p^{n-1}} - p^{k-1} T_{p^{n-2}} & , \quad \text{falls } p \nmid N \\ T_p^n & , \quad \text{falls } p \mid N \end{cases}$$

und

$$T_{nm} = T_n T_m \ \text{ falls } \ (n, m) = 1.$$

Eine Modulform $f(\tau) \in M_k(N)$ heißt **(Hecke-) Eigenfunktion**, falls sie simultane Eigenfunktion unter allen Hecke-Operatoren ist, d.h. falls

$$T(f(\tau)) = \lambda_T f(\tau)$$

für alle Hecke-Operatoren T. Die Zahlen $\lambda_T \in \mathbb{C}$ heißen **Eigenwerte** bezüglich der Hecke-Operatoren T und

$$E_{\lambda_T} := \{f(\tau) \in M_k(N) |\ T(f(\tau)) = \lambda_T f(\tau)\}$$

ist der λ_T-**Eigenraum** bezüglich des Hecke-Operators T.

Sei M ein positiver Teiler von N und d ein positiver Teiler von N/M. Der Automorphismus von $\mathbb{H}$ definiert durch $z \longmapsto d \cdot z$ induziert einen nicht-konstanten Morphismus $t_{M,d} : X_0(N) \longrightarrow X_0(M)$. Falls $g(\tau) \in S_2(M)$ und $M|N$, dann ist $g(d\tau) \in S_2(N)$ für $d|\frac{N}{M}$. Wir bezeichnen mit

$$S_2^{\text{alt}}(N) := \langle g(d\tau) |\ g(\tau) \in S_2(M) \text{ mit } M|N, M \neq N, d|\frac{N}{M} \rangle$$

den Raum der **Altformen** von $S_2(N)$.

Das orthogonale Komplement von $S_2^{\text{alt}}(N)$ bezüglich des **Petersson**-Skalarprodukts

$$\langle f, g \rangle := \int_{\Gamma_0(N)\backslash\mathbb{H}^*} f(\tau)\overline{g(\tau)}dxdy \text{ mit } f, g \in S_2(N), \tau = x + iy$$

bezeichnet man mit $S_2^{\text{neu}}(N)$, und heißt der Vektorraum aller **Neuformen**. Für den Raum $S_2(N)$ der Spitzenformen gilt dann

$$S_2(N) = \bigoplus_{M|N} \bigoplus_{d|N/M} t_{M,d}(S_2^{\text{neu}}(M)).$$

$S_2^{\text{neu}}(N)$ und $S_2^{\text{alt}}(N)$ sind invariant unter allen Hecke-Operatoren, und für den Raum der Neuformen gilt ferner:

Satz 5.1.2 (**Multiplizität 1** [3])**.** $S_2^{\text{neu}}(N)$ besitzt eine Basis aus Eigenfunktionen von T_p $(p \nmid N)$. Die Unterräume, welche von den einzelnen Eigenfunktionen aufgespannt werden, sind alle eindimensional. Jede Eigenform $f \in S_2^{\text{neu}}(N)$ kann normiert werden und besitzt eine Fourier-Entwicklung der Gestalt

$$f(\tau) = q + \sum_{n=2}^{\infty} a_n q^n \quad , \quad q = e^{2\pi i\tau}.$$

Lemma 5.1.3. Sei $f(\tau) = q + \sum_{n=2}^{\infty} a_n q^n \in S_2^{\text{neu}}(N)$ eine Hecke-Eigenform und T ein Hecke-Operator. Dann ist der Hecke-Eigenwert λ_T eine total reelle ganz algebraische Zahl und der Körper

$$K_f := \mathbb{Q}(\lambda_T |\ T \text{ Hecke-Operator})$$

ist eine endliche Erweiterung von $\mathbb{Q}$.

Als eine Konsequenz der durch Deligne [14, 15] bewiesenen Riemannschen Vermutung für Varietäten über endlichen Körpern erhält man den folgenden Satz über die Koeffizienten einer Neuform:

Satz 5.1.3 (**Ramanujan-Petersson-Vermutung).** Für die Koeffizienten der Neuform $f = q + \sum_{n\geq 2} a_n q^n \in S_2^{\text{neu}}(N)$ gilt

$$|a_n| \leq \sigma_0(n)\sqrt{n},$$

wobei $\sigma_0(n)$ die Anzahl der positiven Teiler von n bezeichnet.

Im Rahmen seiner Dissertation hat J. Basmaji [8] einen Algorithmus zur effizienten Berechnung der Hecke-Operatoren implementiert.

Sei $f = q + \sum_{n\geq 2} a_n q^n \in S_2^{\text{neu}}(N)$ eine Neuform und χ ein Dirichlet-Charakter modulo N. Als **Twist** von f bezeichnen wir die eindeutige (normierte) Neuform $f \otimes \chi$ vom Charakter χ^2 mit der Fourier-Entwicklung (siehe [75])

$$f \otimes \chi := q + \sum_{n\geq 2} b_n q^n,$$

wobei $b_p = \chi(p)a_p$ für fast alle Primzahlen p. Demzufolge ist $b_p = \chi(p)a_p$ für alle Primzahlen p mit $(p, \text{cond}(\chi)) = 1$.

Definition 5.1.2. Sei $f = q + \sum_{n\geq 2} a_n q^n \in S_2^{\text{neu}}(N)$ eine Neuform. Ein **innerer Twist** von f ist ein Paar (σ, χ) mit $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ und $\chi \neq 1$ ein Dirichlet-Charakter modulo N, so dass

$$f^\sigma = f \otimes \chi.$$

Die Neuform f besitzt **komplexe Multiplikation**, falls f einen inneren Twist mit trivialem Automorphismus σ besitzt. In diesem Fall ist χ ein Charakter assoziiert zu einem imaginären quadratischen Körper [75]. Den inneren Twist (σ, χ) bezeichnen wir als **extra Twist**, falls σ nicht trivial ist. Die von inneren Twists kommenden Charaktere χ sind stets quadratisch [76]. Besitzt die Neuform $f(\tau) := q + \sum_{n\geq 2} a_n q^n \in S_2^{\text{neu}}(N)$ einen inneren Twist, so gilt $a_p^2 \in \mathbb{Z}$ für alle Primzahlen p.

5.1.3 Arithmetik auf $J_0(N)$

Einfache Faktoren A_f von $J_0^{\text{neu}}(N)$

Definition 5.1.3. Eine über $\mathbb{Q}$ definierte Abelsche Varietät A hat **reelle** Multiplikation, falls $\mathbb{E} := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ ein total reeller Zahlkörper mit maximalem Grad $[\mathbb{E} : \mathbb{Q}] = \dim(A)$ ist. A hat **komplexe** Multiplikation, falls $\mathbb{E} := \text{End}(A) \otimes_{\mathbb{Z}} \mathbb{Q}$ eine total imaginär quadratische Erweiterung eines total reellen Zahlkörpers mit Grad $[\mathbb{E} : \mathbb{Q}] = 2\dim(A)$ ist.

Seien $J_0^{\mathrm{alt}}(N)$ bzw. $J_0^{\mathrm{neu}}(N)$ die durch Altformen bzw. Neuformen erzeugten Untervarietäten von $J_0(N) := \mathrm{Jac}(X_0(N))$, genauer

$$J_0^{\mathrm{alt}}(N) = \prod_{M|N, M\neq N} \prod_{d|N/M} t_{M,d}^* J_0(M) \quad \text{und} \quad J_0^{\mathrm{neu}}(N) = J_0(N)/J_0(N)^{\mathrm{alt}}.$$

Sei $f(\tau) = q + \sum_{n\geq 2} a_n q^n \in S_2^{\mathrm{neu}}(N)$ eine Neuform, $K_f := \mathbb{Q}(a_n |\ n \in \mathbb{N})$ der durch die Fourier-Koeffizienten von f erzeugte Körper, $I_f := \{\sigma_1, \ldots, \sigma_d\}$ die Menge aller verschiedenen Einbettungen von K_f in $\mathbb{C}$ ($d := \#I_f$) und $\{f^{\sigma_1}, \ldots, f^{\sigma_d}\}$ die Menge der zu f konjugierten Neuformen über $\mathbb{Q}$.

G. Shimura hat in [87] zu jeder Neuform $f(\tau) = q + \sum_{n=2}^{\infty} a_n q^n \in S_2^{\mathrm{neu}}(N)$ eine Abelsche Varietät $A_f/\mathbb{Q}$ mit folgenden Eigenschaften konstruiert:

Satz 5.1.4 (**G. Shimura** [87])**.** Zu der Neuform $f(\tau) = q + \sum_{n=2}^{\infty} a_n q^n \in S_2^{\mathrm{neu}}(N)$ existiert eine Abelsche Untervarietät A_f von $J_0(N)$ und ein Isomorphismus θ von K_f nach $\mathrm{End}(A_f) \otimes \mathbb{Q}$ mit

(i) $\dim A_f = [K_f : \mathbb{Q}] = d$,

(ii) Falls $\mathrm{ggT}(n, N) = 1$, dann ist $\theta(a_n)$ die Einschränkung von T_n auf A_f,

(iii) A_f ist über $\mathbb{Q}$ definiert.

Ferner ist (A_f, θ) durch (i), (ii) und (iii) eindeutig bestimmt, und A_f ist eine einfache Abelsche Varietät über $\mathbb{Q}$. Besitzt f keinen inneren Twist, so ist A_f absolut einfach mit reeller Multiplikation, insbesondere ist A_f für quadratfreie Module N absolut einfach.

Bemerkung 5.1.1.

(i) Ist $\chi \neq 1$ ein nicht-trivialer Dirichlet-Charakter und $g = f \otimes \chi \in S_2^{\mathrm{neu}}(N)$ ein Twist von $f \in S_2^{\mathrm{neu}}(N)$, so ist $\chi^2 = 1$. In diesem Fall sind die Abelschen Varietäten A_f und A_g über $\mathbb{Q}$ oder über einem Zahlkörper K mit $[K : \mathbb{Q}] = 2$ isomorph.

(ii) Besitzt die Neuform $f \in S_2^{\mathrm{neu}}(N)$ komplexe Multiplikation, so ist A_f über $\bar{\mathbb{Q}}$ isogen zum Produkt $E^{\dim(A)}$ einer elliptischen Kurve E mit komplexer Multiplikation [85]. Andererseits hat f komplexe Multiplikation, falls A_f einen Faktor mit komplexer Multiplikation besitzt [86].

Für die Neuform $f \in S_2^{\mathrm{neu}}(N)$ gibt es nach Konstruktion einen Morphismus

$$\pi_f \ : J_0^{\mathrm{neu}}(N) \twoheadrightarrow A_f.$$

Für den Pullback von Differentialen gilt

$$\pi_f^*(\Omega^1(A_f)) = S_2(A_f)\ \frac{dq}{q},$$

wobei $S_2(A_f) := \langle f^\sigma : \sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\rangle_{\mathbb{C}}$.

Satz 5.1.5. Sei B_M eine Basis aus nicht-konjugierten Neuformen von $S_2^{\mathrm{neu}}(M)$, dann gilt

$$J_0^{\mathrm{neu}}(N) \sim^{\mathbb{Q}} \prod_{f\in B_N} A_f \quad \text{und} \quad J_0^{\mathrm{alt}}(N) \sim^{\mathbb{Q}} \prod_{M|N, M\neq N} \prod_{f\in B_M} A_f^{\sigma_0(N/M)}.$$

Vermutung 5.1.1 (**Taniyama-Shimura** in verallgemeinerter Fassung)**.**
Es gibt zu jeder einfachen Abelschen Varietät $A/\mathbb{Q}$ mit reeller Multiplikation eine geeignete Stufe $N \in \mathbb{N}$ und eine Neuform $f = q + \sum_{n\geq 2} a_n q^n \in S_2^{\mathrm{neu}}(N)$ mit $A \sim_{\mathbb{Q}} A_f$.

Gruppenordnung der $A_f(\mathbb{F}_p)$

Satz 5.1.6. [88, p. 95-109] Sei A eine Abelsche Varietät über einem Zahlkörper k. Dann gilt für fast alle Primideale $\mathfrak{p}$ des Ganzheitsrings $\mathcal{O}_k$ von k:

(i) Die Reduktion modulo $\mathfrak{p}$ der Abelschen Varietät A definiert eine Abelsche Varietät $\overline{A}$ über dem Restklassenkörper $\mathbb{F}_p$ von $\mathfrak{p}$.

(ii) Es gibt einen injektiven Homomorphismus $\varphi : \mathrm{End}(A) \longrightarrow \mathrm{End}(\overline{A})$.

(iii) Der Grad einer Isogenie bleibt unter dem Homomorphismus φ invariant.

Ein Primideal, für das der obige Satz gilt, heißt Primideal mit **guter Reduktion**.

Ist $C/\mathbb{Q}$ eine Kurve mit reeller Multiplikation, so gilt für die Reduktion der Jacobischen $\mathrm{Jac}(C)$ modulo einem Primideal $\mathfrak{p}$ mit guter Reduktion:

Proposition 5.1.1. ([29, p. 94 - 6.2]) Sei $C/\mathbb{Q}$ eine Kurve mit reeller Multiplikation mit k_0. Sei ferner $\mathfrak{p}$ ein Primideal mit guter Reduktion für $\mathrm{Jac}(C)$. Dann ist die Jacobische der reduzierten Kurve $\overline{C}$ entweder nicht einfach, oder hat komplexe Multiplikation mit einem Erweiterungskörper k von k_0.

Die Operation der Hecke-Operatoren T_p auf $S_2(N)$ induziert einen Endomorphismus auf $J_0(N)$, den wir ebenfalls mit T_p bezeichnen. Hat A_f gute Reduktion modulo p, z.B. für $p \nmid N$, so ergibt sich nach der Eichler-Shimura Theorie [20, 83, 47] für die Reduktion modulo p die Zerlegung

$$T_p = \pi_p + \overline{\pi}_p$$

auf der Jacobischen $J_0(N)/\mathbb{F}_p$ mit dem Frobenius π_p und der Verschiebung $\overline{\pi}_p := p\pi_p^{-1}$. Ist χ_{π_p} das charakteristische Polynom von π_p auf dem l-adischen Tate-Modul (l ist eine Primzahl $\neq p$) von $A_f/\mathbb{F}_p$ und χ_{T_p} das charakteristische Polynom von T_p auf $S_2(A_f)$, so gilt dann

$$x^{\dim(A_f)}\chi_{T_p}(t) = \chi_{\pi_p}(x),$$

wobei $t = x + p/x$. Aus $\#A_f(\mathbb{F}_p) = \chi_{\pi_p}(1)$ sieht man leicht

$$\#A_f(\mathbb{F}_p) = \chi_{T_p}(p+1).$$

Sind ferner a_i genau die Eigenwerte des auf dem Unterraum $S_2(A_f)$ operierenden Hecke-Operators T_p, so gilt

$$\chi_{T_p}(t) = \prod_{i=1}^{2\dim A_f}(1-\alpha_i t) = \prod_{i=1}^{\dim A_f}(1 - a_i t + pt^2).$$

Ist nun A_f über $\mathbb{Q}$ isogen zur Jacobischen $\mathrm{Jac}(C_f)$ einer über $\mathbb{Q}$ definierten Kurve C_f, so gilt

$$\#\mathrm{Jac}(C_f)(\mathbb{F}_p) = \#A_f(\mathbb{F}_p) = \chi_{T_p}(p+1).$$

5.2 Modulare Jacobische der Dimension 3

5.2.1 Nicht-hyperelliptische modulare Kurven vom Geschlecht 3

Definitionen und grundlegende Eigenschaften

Definition 5.2.1. Eine Abelsche Varietät A über einem Zahlkörper K heißt K-**modular der Stufe** N, falls es einen K-Morphismus

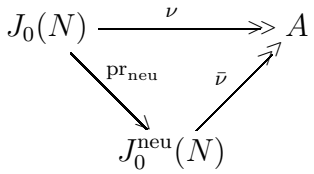
$$\nu \ : J_0(N) \longrightarrow\!\!\!\!\!\rightarrow A$$

zwischen den Abelschen Varietäten $J_0(N)$ und A gibt.
Sei A eine K-modulare Abelsche Varietät der Stufe N.

(i) A heißt K-**neu** (der Stufe N), falls es einen K-Morphismus

$$\bar{\nu} \ : J_0^{\mathrm{neu}}(N) \longrightarrow\!\!\!\!\!\rightarrow A$$

gibt. In diesem Fall ist das folgende Diagram



kommutativ.

(ii) A heißt K-**primitiv** (der Stufe N), falls A für jeden echten Teiler $M|N$ nicht K-modular zur Stufe M ist

Bemerkung 5.2.1. Die Begriffe K-modular, K-neu und K-primitiv kommen ursprünglich aus der Theorie der Modulkurve $X_1(N)$ (siehe [5, 33, 32]), und die von uns verwendeten Begriffe entsprechen genau den K-modularen Abelschen Varietäten mit trivialen Charakter. Wir werden uns nur mit der eingeschränkten Definition von K-modularen Abelschen Varietäten beschäftigen. Die meisten Ergebnisse lassen sich auch auf $X_1(N)$ verallgemeinern.

Definition 5.2.2. Eine glatte projektive Kurve C über einem Zahlkörper K heißt K-**modular** der Stufe N, falls es einen nicht-konstanten Morphismus

$$\pi \ : X_0(N) \longrightarrow C$$

gibt.

Bezeichnung 5.2.1. Wir verwenden die Bezeichnung (A, ν) bzw. (C, π) für die K-modulare Abelsche Varietät A bzw. K-modulare Kurve C mit zugehörigem K-Morphismus ν bzw. π.

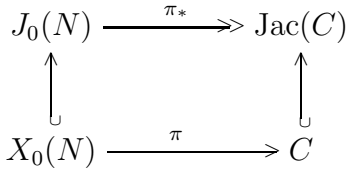
Definition 5.2.3. Eine K-modulare Kurve (C, π) der Stufe N heißt K-**neu** (bzw. K-**primitiv**) der Stufe N, falls ihre Jacobische $\mathrm{Jac}(C)$ K-neu (bzw. K-primitiv) zur Stufe N ist.

Bemerkung 5.2.2 ([5, 32])**.**

(i) Die Modularität ist vom Definitionskörper abhängig.

(ii) Falls (C, π) K-modular ist, so ist $C(K) \neq \emptyset$.

Ist (C, π) K-modular, so ist das folgende Diagramm kommutativ:



Die Umkehrung dieser Aussage ist im allgemeinen falsch.
Ab nun betrachten wir nur noch $\mathbb{Q}$-modulare Abelsche Varietäten (bzw. Kurven), die wir der Einfachheit halber kurz als **modulare** Abelsche Varietäten (bzw. modulare Kurven) bezeichnen werden.
Sei (A, ν) eine neue modulare Abelsche Varietät der Stufe N. Es gibt Neuformen $f_i \in S_2^{\text{neu}}(N)$ mit

$$A \sim_{\mathbb{Q}} A_{f_1} \times \cdots \times A_{f_l}.$$

In diesem Fall gilt

$$\nu^*(\Omega^1(A)) = \bigoplus_{i=1}^{l} S_2(A_{f_i}) \ \frac{dq}{q}.$$

Insbesondere sind neue modulare Abelsche Varietäten auch primitiv der Stufe N. Die Umkehrung ist im allgemeinen falsch.

Proposition 5.2.1 ([32])**.** Sei (A, ν) eine modulare Abelsche Varietät.

(i) Ist A neu der Stufe N, so ist A primitiv der Stufe N.

(ii) Für die $\mathbb{Q}$-einfachen Abelschen Varietäten A sind folgende Aussagen äquivalent

(1) A ist neu der Stufe N
(2) A ist primitiv der Stufe N

Sei $\mathfrak{M}_g$ die Menge der (bis auf $\mathbb{Q}$-Isomorphie) neuen modularen Kurven vom Geschlecht g. Nach Wiles Beweis [101, 92] der Fermatschen Vermutung ist $\#\mathfrak{M}_1$ unendlich. Im Gegensatz zur Klasse der neuen modularen elliptischen Kurven gibt es nur endlich viele neue modulare Kurven vom Geschlecht $g \geq 2$:

Satz 5.2.1 ([33, 5])**.** Die Menge der neuen modularen Kurven vom Geschlecht $g \geq 2$ ist *endlich* und *berechenbar*.

Vermutung 5.2.1 ([5])**.** Die Menge der modularen Kurven vom Geschlecht $g \geq 2$ ist *endlich*.

Der Beweis von Satz 5.2.1 liefert für $g \longrightarrow \infty$ maximal $\exp((6 + o(1))g^2)$ neue modulare Kurven vom Geschlecht g.

Für eine modulare Kurve C mit $\text{Jac}(C) \sim A_f$ benutzen wir die Bezeichnung $S_2(C) := S_2(A_f)$.

Lemma 5.2.1 ([5])**.** Sei C eine neue modulare Kurve vom Geschlecht $g \geq 2$ mit Stufe N. Folgende Aussagen sind äquivalent:

(i) Es gibt einen nicht-konstanten Morphismus $\pi : X_0(N) \longrightarrow C$ mit $S_2(C) \subseteq S_2(X_0(N))^{\text{neu}}$.

(ii) Es gibt einen nicht-konstanten Morphismus $\pi : X_1(N) \longrightarrow C$ mit $S_2(C) \subseteq S_2(X_0(N))^{\text{neu}}$.

(iii) Die Jacobische $\text{Jac}(C)$ der Kurve C ist ein Quotient von $J_0^{\text{neu}}(N)$.

Das folgende Lemma liefert eine Charakterisierung hyperelliptischer modularer Kurven:

Proposition 5.2.2. Sei C eine neue modulare Kurve der Stufe N vom Geschlecht 3. Sei $\{\omega_1, \omega_2, \omega_3\}$ eine Basis von $S_2(C)$ mit Fourier-Entwicklungen $\omega_i = q + \sum_{j\geq 2} a_j^{(i)} q^j$. Dann gilt:

(i) Falls $a_2^{(i)} = a_2^{(j)}$ für alle $1 \leq i, j \leq 3$, so ist C hyperelliptisch und besitzt einen $\mathbb{Q}$-Weierstrass-Punkt P_∞.

(ii) Falls $2|N$, so ist C hyperelliptisch.

(iii) Ist C hyperelliptisch, so besitzt $S_2(C)$ eine Basis $\{f_1, f_2, f_3\}$ mit $F(f_1, f_2, f_3) = 0$ für eine bestimmte Quadrik $F(x, y, z) = 0$.

Beweis. Die Aussagen (i) und (ii) wurden in [5] bewiesen. Die Aussage (iii) folgt aus der Tatsache, dass das Bild $\phi(C)$ von C unter dem kanonischen Morphismus

$$\phi : q \longmapsto (f_1(q) : f_2(q) : f_3(q))$$

eine normale rationale Kurve vom Grad 2 ist. □

Analog zu [5] kann man die nicht-hyperelliptische Variante für modulare Kurven vom Geschlecht 3 beweisen.

Proposition 5.2.3. Sei A ein Quotient der Dimension 3 von $J_0(N)$. Folgende Aussagen sind äquivalent:

(i) Es gibt eine nicht-hyperelliptische modulare Kurve C der Stufe N vom Geschlecht 3, so dass $\text{Jac}(C) \sim_{\mathbb{Q}} A$.

(ii) Es gibt eine nicht-hyperelliptische modulare Kurve C' vom Geschlecht 3 und einen nicht-konstanten Morphismus $\pi' : X_0(N) \longrightarrow C'$, so dass $\pi'^*(\Omega^1(C')) = \Omega^1(A)$.

(iii) $S_2(A)$ besitzt eine Basis $\{f_1, f_2, f_3\}$ mit $F(f_1, f_2, f_3) = 0$ für eine (bis auf Isomorphie) bestimmte glatte Quartik $F(x, y, z) = 0$.

Sei C eine nicht-hyperelliptische modulare Kurve vom Geschlecht 3. Nimmt man eine ganzzahlige Basis von $S_2(A)$, so ist die in Proposition 5.2.3 erwähnte Quartik über $\mathbb{Q}$ definiert.

Lemma 5.2.2. Sei (C, π) eine nicht-hyperelliptische modulare Kurve vom Geschlecht 3 mit $\pi^*(\Omega^1(C)) = \Omega^1(A_f)$ für eine Neuform $f \in S_2^{\text{neu}}(N)$. $S_2(A_f)$ besitzt eine Basis $\{h_1, h_2, h_3\}$ mit

$$h_1 = q + O(q^2), \quad h_2 = q^2 + O(q^3), \quad h_3 = O(q^3).$$

Bezüglich der kanonischen Einbettung

$$\phi : q \longmapsto (h_1(q) : h_2(q) : h_3(q))$$

ist $\phi(C)$ eine glatte Quartik mit $P_\infty = (1 : 0 : 0) \in \phi(C)(\mathbb{Q})$. Der Punkt P_∞ ist ein Weierstrass-Punkt erster (bzw. zweiter) Ordnung genau dann, wenn $h_3 = q^4 + O(q^5)$ (bzw. $h_3 = O(q^5)$).

Beweis. Sei $S_2(A_f) = \langle f, f^\sigma, f^{\sigma^2} \rangle$ mit $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Wegen Proposition 5.2.2 ist $a_2 \notin \mathbb{Q}$, und somit besitzt $S_2(A_f)$ durch Gauß-Elimination eine Basis $\{h_1, h_2, h_3\}$ mit

$$h_1 = q + O(q^2), \quad h_2 = q^2 + O(q^3), \quad h_3 = O(q^3).$$

Da C modular und nicht-hyperelliptisch vom Geschlecht 3 ist, ist das Bild $\phi(C)$ von C unter der kanonischen Einbettung ϕ

$$\phi : q \longmapsto (h_1(q) : h_2(q) : h_3(q))$$

eine glatte Quartik der Gestalt

$$\sum a_{ijk} x^i y^j z^k = 0. \tag{5.1}$$

Setzt man $x := h_1(q), y := h_2(q)$ und $z := h_3(q)$, und berechnet man die Monome $x^i y^j z^k$, so gilt $x^4 = q^4 + O(q^5)$, $x^3 y = q^5 + O(q^6)$, und $x^i y^j z^k = O(q^6)$ sonst.
In (5.1) gilt dann $a_{400}, a_{310} = 0$ und somit ist $P_\infty := (1 : 0 : 0) \in \phi(C)(\mathbb{Q})$. Die Tangente l_∞ an P_∞ ist die Gerade mit der Gleichung $z = 0$. Ist ferner $h_3(q) = O(q^4)$, so gilt $x^2 y^2 = q^6 + O(q^7)$ und $x^i y^j z^k = O(q^7)$ für die von x^2y^2, x^4, x^3y verschiedenen Monomen. Demzufolge ist $a_{220} = 0$. $\phi(C)$ besitzt dann eine Gleichung der Form

$$\begin{aligned} F(x,y,z) \;=\; & x^3 z + x^2(a_{211} yz + a_{202} z^2) + x(a_{130} y^3 + a_{121} y^2 z + a_{112} y z^2 + a_{103} z^3) \\ & + (a_{040} y^4 + a_{031} y^3 z + a_{022} y^2 z^2 + a_{013} y z^3 + a_{004} z^4) = 0 \end{aligned}$$

und somit ist P_∞ ein Weierstrass-Punkt erster Ordnung.
Der Beweis für einen Weierstrass-Punkt zweiter Ordnung erfolgt analog: Man erhält für $h_3 = O(q^5)$ die Gleichungen $x^2y^2 = q^6 + O(q^7),\ xy^3 = q^7 + O(q^8)$ und $x^iy^jz^k = O(q^8)$ für die Monome verschieden von x^2y^2, x^4, x^3y, xy^3, und somit gilt $a_{220} = a_{130} = 0$, woraus die Behauptung folgt. □

Berechnung der nicht-hyperelliptischen neuen modularen Kurven vom Geschlecht 3 zu den Stufe $N \leq 4000$

Nun betrachten wir nur die nicht-hyperelliptischen neuen modularen Kurven C vom Geschlecht 3, die über $\mathbb{Q}$ eine einfache Jacobische Varietät $A \sim_{\mathbb{Q}} \mathrm{Jac}(C)$ besitzen. In diesem Fall gibt es eine Neuform $f = q + \sum_{n=2}^{\infty} a_n q^n \in S_2^{\mathrm{neu}}(N)$ mit $\mathrm{Jac}(C) \sim_{\mathbb{Q}} A_f$.

Sei $\{f_1, f_2, f_3\}$ eine Basis von $S_2(A_f)$ bestehend aus Spitzenformen mit ganzzahligen Fourier-Koeffizienten und sei

$$N_4 := \{f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3} |\ \alpha_1 + \alpha_2 + \alpha_3 = 4\} =: \{F_1, \ldots, F_{15}\}$$

die Menge aller Monome $f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3}$ vom Grad 4. Die Elemente von N_4 sind Spitzenformen vom Gewicht 8. Unter allen Spitzenformen

$$\sum_{i=1}^{15} a_i F_i,\ a_i \in \mathbb{Z}$$

vom Gewicht höchstens 8 entspricht die Gleichung von C genau der trivialen Spitzenform. Seien nun die Fourier-Entwicklungen

$$F_i = \sum_{j=1}^{\infty} b_{ij} q^j.$$

Die Spitzenform

$$F = \sum_{i=1}^{15} a_i F_i = \sum_{j=1}^{\infty} \left(\sum_{i=1}^{15} b_{ij} a_i \right) q^j$$

ist nach Satz 5.1.1 genau dann gleich 0, wenn

$$\sum_{i=1}^{15} b_{ij} a_i = 0 \text{ für alle } j \leq \mu k/12 =: m \text{ mit } \mu = N \prod_{p|N} (1 + p^{-1}) \text{ und } k = 8.$$

Die Lösung dieses linearen Gleichungssystems liefert uns eine Linearkombination des Nullverktors bezüglich der Spalten der Matrix $B = (b_{ij})$. Da die Spalten von B genau die (Fourier-Koeffizienten der) Monome $f_1^{\alpha_1} f_2^{\alpha_2} f_3^{\alpha_3}$ vom Grad 4 sind, entspricht C genau der Lösung des obigen linearen Gleichungssystems. In der Praxis braucht man nicht alle Spalten der Matrix B zu betrachten. Meistens genügt es schon mit weniger Spalten das lineare Gleichungssystem zu lösen. Leicht verifiziert man dann, ob die entstandene Relation tatsächlich der trivialen Spitzenform entspricht.

Zur Arithmetik der Modulkurven verwenden wir das umfangreiche Programmpaket MAGMA [60] sowie MAV [35]. Dadurch war es möglich, folgende Aufgaben zu lösen

- Untersuchung des Zerlegungsverhaltens der Jacobischen $J_0(N)$ in einfache Faktoren,
- Berechnung der Fourier-Entwicklungen von Spitzenformen $f \in S_2^{\text{neu}}(N)$,
- Berechnungen von Periodenmatrizen der einfachen Faktoren A_f (siehe Abschnitt 5.2.2),
- Berechnung der Schnittpaarung H_f (siehe Abschnitt 5.2.2).

Für das folgende Beispiel benutzen wir den Ausdruck $A^{(i)}$, um eine Abelsche Varietät A der Dimension i zu bezeichnen.

Beispiel 5.2.1. Sei $N = 203$. Die Modulkurve $X_0(203)$ hat Geschlecht 19. Der zu $S_2^{\text{neu}}(203)$ gehörende Teil $J_0^{\text{neu}}(203)$ der Jacobischen $J_0(203)$ hat Dimension 15 und zerfällt in

$$J_0^{\text{neu}}(203) \sim A_1^{(1)} \times A_2^{(1)} \times A_3^{(1)} \times A_4^{(2)} \times A_5^{(2)} \times A_6^{(3)} \times A_7^{(5)}$$

mit von neuen Spitzenformen $f \in S_2^{\text{neu}}(203)$ erzeugten j-dimensionalen Abelschen Varietäten $A_i^{(j)}$. Die 3-dimensionale Abelsche Varietät $A_6^{(3)}$ kommt aus der Spitzenform f mit der Fourier-Entwicklung

$$\begin{aligned} f(q) &= q + \alpha q^2 + (-\alpha^2 - \alpha + 1)q^3 + (\alpha^2 - 2)q^4 + (\alpha^2 - 4)q^5 + (-2\alpha - 1)q^6 \\ &\quad -q^7 + (-\alpha^2 - \alpha + 1)q^8 + (\alpha^2 + 2\alpha - 1)q^9 + O(q^{10}) \end{aligned}$$

wobei $\alpha^3 + \alpha^2 - 3\alpha - 1 = 0$. Der Raum $S_2(A_f)$ wird dann von den Spitzenformen

$$\begin{aligned} f_1(q) &= q - q^4 - 3q^5 - q^6 - q^7 + O(q^{10}) \\ f_2(q) &= q^2 - q^4 - q^5 - 2q^6 + q^9 + O(q^{10}) \\ f_3(q) &= q^3 - q^4 - q^5 + q^8 - q^9 + O(q^{10}) \end{aligned}$$

mit ganzzahligen Koeffizienten erzeugt. Mittels Lemma 5.2.2 berechnen wir die Gleichung der modularen Kurve C^F_{203}

$$\begin{aligned} C^F_{203} \; : \quad & x^3z - x^2y^2 - 3x^2z^2 + xy^3 + 3xy^2z - 4xyz^2 + 4xz^3 - y^4 + 3y^3z \\ & -6y^2z^2 + 3yz^3 - 2z^4 = 0 \end{aligned}$$

mit $\mathrm{Jac}(C^F_{203}) \sim_{\mathbb{Q}} A_{3,1}$.

Bemerkung 5.2.3. In allen betrachteten Beispielen haben wir jedoch nicht versucht, die Koeffizienten der Kurvengleichung zu minimieren.

Wir benutzen den in [34] definierten Vorgang zur Etikettierung der Neuformen, welcher insbesondere eine Ordnung zwischen (Galois-konjugierten Klassen von) Neuformen mit vorgegebener Stufe definiert.

C^B_{109}	$x^3z - 2x^2yz - x^2z^2 - xy^3 + 6xy^2z - 6xyz^2 + 3xz^3 + y^4 - 6y^3z$ $+10y^2z^2 - 5yz^3 = 0$
C^A_{151}	$x^3z - 2x^2yz - 2x^2z^2 - xy^3 + 2xy^2z + 4xyz^2 + xz^3 + y^2z^2 - 3yz^3 - 2z^4 = 0$
C^B_{179}	$x^3z - 2x^2yz - 2x^2z^2 - xy^3 + 2xy^2z + xyz^2 + 2xz^3 + y^2z^2 - yz^3 - z^4 = 0$
C^A_{295}	$x^3z - x^2y^2 - x^2z^2 + xy^3 - xy^2z + 2xyz^2 - xz^3 - y^3z + 3y^2z^2 - yz^3 = 0$
C^F_{369}	$x^3z - 2x^2z^2 - xy^3 + 6xyz^2 - 6xz^3 - 3y^2z^2 + 6yz^3 - z^4 = 0$
C^L_{855}	$x^3z - x^2z^2 - xy^3 + 3xyz^2 - 3xz^3 + 2y^3z - 3y^2z^2 + 3yz^3 = 0$
C^P_{1215}	$x^3z - xy^3 + 3xyz^2 + 5xz^3 - 6y^2z^2 - 3yz^3 + z^4 = 0$

Tabelle 5.1: Modulare Kurven (mit $\mathbb{Q}$-rationalen Weierstrass-Punkten) und mit $\mathbb{Q}$-einfachen Jacobischen, $N \leq 4000$

C_{97}^{A}	$x^3z - x^2y^2 - 5x^2z^2 + xy^3 + xy^2z + 3xyz^2 + 6xz^3 - 3y^2z^2 - yz^3 - 2z^4 = 0$
C_{113}^{C}	$x^3z - x^2y^2 - 4x^2z^2 + xy^3 + 2xy^2z + 6xz^3 - y^3z - 3y^2z^2 + yz^3 - 3z^4 = 0$
C_{127}^{A}	$x^3z - x^2y^2 - 3x^2z^2 + xy^3 - xyz^2 + 4xz^3 + 2y^3z - 3y^2z^2 + 3yz^3 - 2z^4 = 0$
C_{139}^{B}	$x^3z - x^2y^2 - 2x^2z^2 + xy^3 - 2xy^2z + 2xyz^2 + xz^3 + y^4 - 2y^3z$ $+4y^2z^2 - 3yz^3 = 0$
C_{149}^{A}	$x^3z - x^2y^2 - 3x^2z^2 + xy^3 + 3xy^2z - 2xyz^2 + 2xz^3 - y^4 - y^2z^2 + yz^3 = 0$
C_{169}^{C}	$x^3z - x^2y^2 - 3x^2z^2 + xy^3 + 2xyz^2 + xz^3 + y^2z^2 - 3yz^3 + z^4 = 0$
C_{187}^{E}	$x^3z - x^2y^2 - x^2z^2 + xy^3 - xy^2z - xyz^2 + 2xz^3 + y^3z - y^2z^2 + 3yz^3 = 0$
C_{203}^{F}	$x^3z - x^2y^2 - 3x^2z^2 + xy^3 + 3xy^2z - 4xyz^2 + 4xz^3 - y^4 + 3y^3z - 6y^2z^2$ $+3yz^3 - 2z^4 = 0$
C_{217}^{A}	$3x^3z - 3x^2y^2 - 11x^2z^2 - 3xy^3 + 13xy^2z - 2xyz^2 + 11xz^3 - 2y^4 - y^3z$ $-4y^2z^2 + yz^3 - 2z^4 = 0$
C_{239}^{A}	$x^3z - x^2y^2 - x^2z^2 + xy^3 - xy^2z + xz^3 + y^4 - y^3z + yz^3 - z^4 = 0$
C_{243}^{E}	$x^3z - 3x^2z^2 - xy^3 + 9xyz^2 - 6xz^3 + 2y^3z - 9y^2z^2 + 9yz^3 - 2z^4 = 0$
C_{329}^{D}	$x^3z - x^2y^2 + xy^3 + xyz^2 + xz^3 - y^3z + 2yz^3 + z^4 = 0$
C_{475}^{H}	$x^3z - x^2y^2 - 5x^2z^2 - xy^3 + xy^2z + 17xyz^2 + 14xz^3 - 2y^4 - 14y^3z$ $-35y^2z^2 - 35yz^3 - 12z^4 = 0$
C_{1175}^{D}	$x^3z - x^2y^2 + x^2z^2 + xy^3 - 2xy^2z + 2xyz^2 - xz^3 + y^4 - 2y^3z + y^2z^2 + yz^3 = 0$

Tabelle 5.2: Modulare Kurven (ohne $\mathbb{Q}$-rationale Weierstrass-Punkte) mit $\mathbb{Q}$-einfachen Jacobischen, $N \leq 4000$

Nicht-neue modulare Kurven und modulare Kurven mit nicht $\mathbb{Q}$-einfachen Jacobischen

Die für uns interessante modulare Kurven angesichts ihrer Anwendung in der Kryptographie müssen eine $\mathbb{Q}$-einfache Jacobische haben. Modulare Jacobische, die über $\mathbb{Q}$ zerfallen, sind für die Kryptographie ungeeignet. Dennoch werden wir sie im folgenden untersuchen, nicht wegen ihre Anwendung in der Kryptographie, sondern um die in Lemma 5.2.2 vorgestellte Methode vollständig zu behandeln.

Sei C eine nicht-hyperelliptische modulare Kurve vom Geschlecht 3. Ist C neu, so lässt sich Lemma 5.2.2 direkt anwenden. Ist C nicht-neu, so liegt der einzige Unterschied in der Berechnung der zugrundliegenden Basis:

Lemma 5.2.3. ([5, Lemma 3.6]) Sei $\pi : X_0(N) \longrightarrow C$ ein nicht-konstanter $\mathbb{Q}$-Morphismus. Dann besitzt $S_2(C)$ eine $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$-invariante Basis B bestehend aus Spitzenformen

$$h(q) = \sum_{d|N/M} c_d f(q^d)$$

für ein $M|N$, $f \in S_2^{\mathrm{neu}}(M)$ und $c_d \in K_f$.

Beispiel 5.2.2. Sei $N = 178 = 2 \cdot 89$. Die Jacobische $J_0(178)$ zerfällt über $\mathbb{Q}$ in $J_0(178) = J_0^{\mathrm{neu}}(178) \times J_0^{\mathrm{alt}}(178)$ mit $J_0^{\mathrm{neu}}(178) = A_{f_1}^{(1)} \times A_{f_2}^{(1)} \times A_{f_3}^{(2)} \times A_{f_4}^{(3)}$ und $J_0^{\mathrm{alt}}(178) = (B_{g_1}^{(1)})^2 \times (B_{g_2}^{(1)})^2 \times (B_{g_3}^{(5)})^2$. Sei A_{f_3,g_2} die nicht-einfache und nicht-neue Abelsche Varietät $A_{f_3}^{(2)} \times B_{g_2}^{(1)}$ der Dimension 3 mit den Spitzenformen

$$\begin{aligned} f_3(q) &= q + q - q^2 + aq^3 + q^4 + (-2a-3)q^5 + O(q^6) \in S_2^{\mathrm{neu}}(178), \\ g_2(q) &= q - q^2 - q^3 - q^4 - q^5 + O(q^6) \in S_2^{\mathrm{neu}}(89), \end{aligned}$$

wobei $K_{f_3} = \mathbb{Q}(a)$ mit $a^2 + 2a - 1 = 0$. Sei $\{f_{31}, f_{32}\}$ die ganzzahlige Basis von $S_2(A_{f_3})$

$$\begin{aligned} f_{31}(q) &= q - q^2 + q^4 - 3q^5 - 2q^7 - q^8 - 2q^9 + O(q^{10}), \\ f_{32}(q) &= q^3 - 2q^5 - q^6 - 2q^9 + O(q^{10}). \end{aligned}$$

Dann gibt es eine glatte Quartik $C : F = 0$ mit

$$F(f_{31}(q), f_{32}(q), g_2(q) + 2g_2(q^2)) = 0,$$

nämlich die Kurve mit der Gleichung

$$F(x,y,z) = x^4 - 8x^3y + 38x^2y^2 - 2x^2z^2 - 24xy^3 - 8xyz^2 - 7y^4 + 6y^2z^2 + z^4$$

Die Kurve C ist also eine nicht-hyperelliptische nicht-neue modulare Kurve vom Geschlecht 3.

Sei wiederum $f \in S_2^{\text{neu}}(N)$ mit $\dim(A_f) = 3$ und $\{f_1, f_2, f_3\}$ eine Basis von $S_2(A_f)$ bestehend aus Spitzenformen mit ganzzahligen Fourier-Koeffizienten. Gibt es ein homogenes Polynom $F \in \mathbb{Q}[x, y, z]$ vom Grad $d \geq 5$ mit $F(f_1, f_2, f_3) = 0$, so dass die Kurve $C : F = 0$ vom Geschlecht 3 ist, so ist der Funktionenkörper $\mathbb{Q}(\phi(C))$ der kanonischen Einbettung von C in $\mathbb{Q}(X_0(N))$ enthalten. Da $C' := \phi(C)$ eine glatte Quartik ist, existiert ein nicht-konstanter $\mathbb{Q}$-Morphismus $\pi : X_0(N) \longrightarrow C'$. In diesem Fall ist $\text{Jac}(C')$ entweder nicht-neu oder neu für einen Teiler M von N.

Beispiel 5.2.3. Wir beziehen uns auf Beispiel 5.2.2 und betrachten die einfache Abelsche Varietät $A_{f_4}^{(3)}$ der Dimension 3. Bezüglich der ganzzahlige Basis $\{f_{41}, f_{42}, f_{43}\}$ von $S_2(A_{f_4})$ aus Spitzenformen

$$\begin{aligned} f_{41}(q) &= q + q^2 + q^4 + q^8 + 3q^9 + O(q^{10}), \\ f_{42}(q) &= q^3 - q^5 + q^6 - q^9 + O(q^{10}), \\ f_{43}(q) &= q^7 - 2q^9 + O(q^{10}) \end{aligned}$$

berechnet man die Gleichung einer nicht-hyperelliptische Kurve vom Geschlecht 3 mit dem Modell

$$\begin{aligned} C: \quad 0 = \; & x^5z^2 - 3x^4yz^2 + 8x^4z^3 - 2x^3y^3z + 7x^3y^2z^2 - 23x^3yz^3 + 26x^3z^4 \\ & -3x^2y^3z^2 + 18x^2y^2z^3 - 53x^2yz^4 + 42x^2z^5 + xy^6 - 3xy^5z - y^7 \\ & +xy^4z^2 + 14xy^3z^3 - 10xy^2z^4 - 36xyz^5 + 32xz^6 + 4y^6z + 10y^5z^2 \\ & -66y^4z^3 + 124y^3z^4 - 100y^2z^5 + 20yz^6 + 8z^7. \end{aligned}$$

Ihre kanonische Einbettung kann mittels MAGMA ermittelt werden: sie besitzt die Gleichung

$$\begin{aligned} C': \quad 0 = \; & x^4 - 4x^3y + 6x^3z + 2x^2y^2 - 5x^2z^2 + 4xy^3 - 30xy^2z \\ & +64xyz^2 - 42xz^3 - 3y^4 + 8y^3z + 9y^2z^2 - 40yz^3 + 28z^4. \end{aligned}$$

Nun kann man leicht überprüfen, dass $\text{Jac}(C')$ isogen zur Abelschen Varietät A_{f_3,g_2} aus Beispiel 5.2.2 ist.

Im allgemeinen sind $\text{Jac}(C')$ und A_f nicht isogen. Ist aber $\text{Jac}(C')$ $\mathbb{Q}$-einfach und neu, so gibt es eine Neuform $g \in S_2^{\text{neu}}(N)$ mit $\text{Jac}(C') \sim_{\mathbb{Q}} A_g$. Ist in diesem Fall $g^\sigma = f \otimes \chi$ für $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ und χ einen Dirichlet-Charakter, so ist $A_f \sim_K \text{Jac}(C')$, für einen Zahlkörper K vom Grad 2.

Beispiel 5.2.4. Sei $N = 243 = 3^5$. Der zu $S_2^{\text{neu}}(243)$ gehörende Teil $J_0^{\text{neu}}(243)$ der Jacobischen $J_0(243)$ hat Dimension 12 und zerfällt in

$$J_0^{\text{neu}}(243) \simeq A_{f_1}^{(1)} \times A_{f_2}^{(1)} \times A_{f_3}^{(2)} \times A_{f_4}^{(2)} \times A_{f_5}^{(3)} \times A_{f_6}^{(3)}$$

mit den durch neue Spitzenformen $f_j \in S_2^{\text{neu}}(N)$ erzeugten j-dimensionalen Abelschen Varietäten $A_{f_i}^{(j)}$. Die 3-dimensionale Abelsche Varietät $A_{f_6}^{(3)}$ kommt aus der Spitzenform mit der Fourier-Entwicklung

$$f_6(q) \;=\; q + \alpha q^2 + (\alpha^2 - 2)q^4 + (-\alpha + 3)q^5 + (-2\alpha^2 + 3\alpha + 2)q^7 + O(q^8),$$

wobei $\alpha^3 - 3\alpha^2 + 3 = 0$. Wie zuvor berechnet man eine Basis $\{f_{61}, f_{62}, f_{63}\}$ von $S_2(A_{f_6})$

$$\begin{aligned} f_{61}(q) &= q + 3q^5 - 2q^7 + 3q^8 + O(q^{10}), \\ f_{62}(q) &= q^2 - q^5 + 3q^7 - 4q^8 + O(q^{10}), \\ f_{63}(q) &= q^4 - 2q^7 + 3q^8 + O(q^{10}), \end{aligned}$$

bestehend aus Spitzenformen mit ganzzahligen Fourier-Koeffizienten. Sei nun C die singuläre Kurve vom Geschlecht 3 und Grad $d = 6$ gegeben durch die Gleichung

$$\begin{aligned} C \;:\quad & x^5z - 7x^4z^2 - x^3y^3 - 9x^3yz^2 + x^3z^3 + 6x^2y^3z + 9x^2y^2z^2 \\ & + 27x^2yz^3 + 19x^2z^4 - 3xy^3z^2 + 18xy^2z^3 + 27xyz^4 + 2xz^5 \\ & + 8y^3z^3 + 9y^2z^4 - 9yz^5 - 8z^6 = 0. \end{aligned}$$

Dann ist $F(f_{61}(q), f_{62}(q), f_{63}(q)) = 0$. Die kanonische Einbettung von C ist die glatte Quartik C' mit der Gleichung

$$\begin{aligned} C' \;:\quad & x^3y - 2x^3z - 12x^2y^2 + 9x^2yz - 24x^2z^2 + 48xy^3 + 24xy^2z \\ & - 57xyz^2 + 66xz^3 - 64y^4 + 104y^3z - 36y^2z^2 - 65yz^3 + 88z^4 = 0. \end{aligned}$$

C' ist eine neue modulare Kurve mit $\mathbb{Q}$-einfacher Jacobischer $\text{Jac}(C') \sim A_{f_5}$, wobei

$$f_5(q) \;=\; q + \beta q^2 + (\beta^2 - 2)q^4 + (-\beta - 3)q^5 + (-2\beta^2 - 3\beta + 2)q^7 + O(q^8)$$

und mit $\beta^3 + 3\beta^2 - 3 = 0$. Da es ein $\sigma \in \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ und einen nicht-trivialen Dirichlet-Charakter χ mit $f_6^\sigma = f_5 \otimes \chi$ gibt, ist $A_{f_6} \sim_K A_{f_5}$ für einen quadratischen Zahlkörper K.

5.2.2 Nicht-hyperelliptische modulare Jacobische A_f der Dimension 3

In diesem Abschnitt werden wir uns nur noch mit modularen (absolut-) einfachen Abelschen Varietäten der Dimension 3, die prinzipal polarisiert sind, beschäftigen. In diesem Fall sind sie auch Jacobische von Kurven des Geschlechts 3. Durch die Berechnung der Thetanullwerte kann man leicht entscheiden, ob die entsprechende Kurve C hyperelliptisch oder nicht-hyperelliptisch ist.

Wir haben im Rahmen dieser Arbeit das Verhalten der Abelschen Varietäten A_f der Dimension 3 für $N \leq 4000$ untersucht. Die unten abgebildete Tabelle liefert uns die Anzahl der aufgetretenen prinzipal polarisierten Abelschen Varietäten, hyperelliptischen Jacobischen und nicht-hyperelliptischen Jacobischen.

$\#A_f$	3334
# p.p. A_f	79
$\#A_f \in \mathrm{Jac}(\mathcal{H}_3(k))$	12
# p.p. $A_f \notin \mathrm{Jac}(\mathcal{H}_3(k))$	67

Tabelle 5.3: Verhalten der A_f mit $\dim A_f = 3$ und $N \leq 4000$

Periodenmatrizen der A_f

Wir beschreiben in diesem Abschnitt eine Methode von Wang [96] um zu entscheiden ob die Abelsche Varietät A_f prinzipal polarisiert ist oder nicht.

Sei $f = q + \sum_{n\geq 2} a_n q^n \in S_2^{\mathrm{neu}}(N)$ eine Neuform und die dazugehörige Abelsche Varietät A_f. Sei $\mathbf{f} := (f^{\sigma_1}, \ldots, f^{\sigma_d})^t$ und $\omega(\mathbf{f}) := (\omega(f^{\sigma_1}), \ldots, \omega(f^{\sigma_d}))^t$. Das Bild von $H_1(X_0(N), \mathbb{Z})$ unter der Abbildung

$$H_1(X_0(N), \mathbb{Z}) \ni \gamma \longmapsto \int_\gamma \omega(\mathbf{f}) := (\int_\gamma \omega(f^{\sigma_1}), \ldots, \int_\gamma \omega(f^{\sigma_d}))^t \in \mathbb{C}^d$$

ist ein freier $\mathbb{Z}$-Modul vom Rang $2d$, also mit anderen Worten ein Gitter Λ_f in $\mathbb{C}^d$.

Die Abelsche Varietät A_f ist dann isomorph zum Torus $\mathbb{C}^d/\Lambda_f$ mit der Schnittpaarung H_f in $H_1(X_0(N), \mathbb{Z})$

$$H_f : H_1^+(X_0(N), \mathbb{Z}) \times S_2(N) \ni (\sigma, f) \longmapsto H_f(\sigma, f) := \int_\sigma \omega(f) \in \mathbb{C}$$

als nicht-degenerierte Hermitesche Form auf Λ_f und

$$\Im\mathrm{m}(H_f(\Lambda_f, \Lambda_f)) \subset \mathbb{Z}.$$

$\Im\mathrm{m}(H_f)$ ist dann eine Riemannform auf Λ_f. Sei ferner $\{w_1, \ldots, w_{2d}\}$ eine symplektische Basis von Λ_f. Dann existieren positive ganze Zahlen $e_1, \ldots, e_d$ mit $e_1|e_2|\cdots|e_d$, so dass

$$(\Im\mathrm{m}(H_f(w_i, w_j)))_{i,j=1,\ldots,2d} = \begin{pmatrix} 0 & \Delta_f \\ -\Delta_f & 0 \end{pmatrix}$$

mit einer Diagonalmatrix

$$\Delta_f = \begin{pmatrix} e_1 & & \\ & \ddots & \\ & & e_d \end{pmatrix}.$$

Satz 5.2.2 ([96])**.** Seien

$$A_f := \left(\int_{w_i} \omega(f^{\sigma_j}) \right)_{i,j=1,\ldots,d} \in \mathbb{C}^{d\times d}$$

und

$$B_f := \left(\int_{w_i} \omega(f^{\sigma_j}) \right)_{\substack{i=d+1,\ldots,2d \\ j=1,\ldots,d}} \in \mathbb{C}^{d\times d}.$$

Dann gilt für die Periodenmatrix Ω_f (bis auf die Operation der symplektischen Gruppe $\mathrm{Sp}(2d, \mathbb{Z})$ auf $\mathbb{H}_d$)

$$\Omega_f = e_d A_f^{-1} B_f \Delta_f^{-1}.$$

Insbesondere ist A_f $\mathbb{Q}$-isogen zu einer prinzipal polarisierten Abelschen Varietät falls $e_1 = \cdots = e_d$.

Nicht-hyperelliptische modulare Jacobische A_f der Dimension 3

Als Abelsche Varietät vom GL_2-Typ besitzen die prinzipal polarisierbaren Varietäten A_f genau

$$2^M, \quad \text{mit} \quad 0 \leq M \leq [K_f : \mathbb{Q}] - 1$$

Isomorphieklassen von prinzipalen Polarisierungen über $\mathbb{Q}$ (siehe [31]).

Hier betrachten wir nur die (bezüglich der kanonischen Polarisierung H_f) prinzipal polarisierten Abelschen Varietäten A_f. Nach dem vorherigen Abschnitt ist man in der Lage, die Periodenmatrix Ω_f von A_f als 3-dimensionalen komplexen

Torus zu berechnen, sowie zu untersuchen ob A_f bezüglich H_f prinzipal polarisiert ist.
Ab nun betrachten wir nur die A_f, die prinzipal polarisiert sind. Aus der Kenntnis von Ω_f (und somit ihrer geraden Thetanullwerte) entscheidet man leicht, welche der A_f Jacobische von nicht-hyperelliptischen Kurven sind. Ist $A_f \simeq \mathrm{Jac}(C_f)$ für eine nicht-hyperelliptische Kurve C_f vom Geschlecht 3, so berechnet man mit der in Kapitel 4 beschriebene Methode die Bitangenten von C_f und somit ein Riemann-Modell von C_f über $\mathbb{C}$.

Der natürliche Weg, um die Gleichung über $\bar{\mathbb{Q}}$ zu rekonstruieren, wäre, von den $\mathbb{Q}$-Invarianten glatter Quartiken die Gleichung mittels Gröbner-Basen zu ermitteln. Ein vollständiges Invariantensystem für glatten Quartiken ist allerdings bis heute nicht bekannt. Im folgenden werden wir nur die prinzipal polarisierten modularen Abelschen Varietäten $A_f \simeq \mathrm{Jac}(C_f)$ sowie die Dixmier-Invarianten von C_f auflisten.

Details zur nummerischen Approximation der $i_1, \ldots, i_6$

Um die nötige Genauigkeit zur Berechnung der Periodenmatrix Ω_f (bezüglich der kanonischen Polarisierung H_f) von A_f zu erreichen, benötigen wir genügend viele Fourier-Koeffizienten der neuen Eigenform $f \in S_2^{\mathrm{neu}}(N)$. Für unsere Berechnungen betrachteten wir die 20000 ersten Fourier-Koeffizienten.
Für $\mathbb{Q}$-einfache modulare Jacobische $A_f \simeq \mathrm{Jac}(C_f)$ sind die entsprechenden Dixmier-Invarianten von C_f auch über $\mathbb{Q}$ definiert, C_f könnte selbst über einem Zahlkörper (vom Grad ≥ 1) definiert sein. Ist C_f über $\mathbb{Q}$ definiert, so würde man erwarten, dass C_f ein Modell mit relativ kleinen Koeffizienten besitzt. Um den Vorteil dieser kleinen Koeffizienten ausnutzen zu können, berechnen wir nicht die in Kapitel 3 dargestellten Invarianten, sondern

$$i'_1 = \frac{I_6}{I_3^2}, \quad i'_2 = \frac{I_9}{I_3^3}, \quad i'_3 = \frac{I_{12}}{I_3^4}, \quad i'_4 = \frac{I_{15}}{I_3^5}, \quad i'_5 = \frac{I_{18}}{I_3^6}, \quad i'_6 = \frac{I_{27}}{I_3^9}$$

mit noch kleineren Koeffizienten. Im generischen Fall ist auch $I_3 \neq 0$.
Dadurch ist es recht einfach die berechneten komplexwertigen Invarianten durch rationale Zahlen zu approximieren, zumindest für i'_1. Für unsere Berechnungen haben wir dafür die Magma-Funktion

```
BestApproximation(x,10^a)
```

mit einem geeignet gewählten $a \in \mathbb{N}$ benutzt. Ebenso könnte man auch direkt versuchen, die anderen Invarianten $i'_2, \ldots, i'_6$ mit rationalen Zahlen zu approximieren. Eine Alternative (nach der Approximation von i'_1 durch die rationale Zahl $\frac{I_6}{I_3^2}$) wäre

$$i'_2 I_3^3 =: \tilde{I}_9,\ i'_3 I_3^4 =: \tilde{I_{12}},\ i'_4 I_3^5 =: \tilde{I_{15}},\ i'_5 I_3^6 =: \tilde{I_{18}},\ i'_6 I_3^9 =: \tilde{I_{27}}$$

ganzzahlig anzunähern.
Ein naiver Ansatz für die Suche nach besseren Annäherungen von i'_6 basiert auf einer Eigenschaft von Diskriminanten glatter Quartiken: Ist C_f über $\mathbb{Z}$ definiert, so besitzt ihre Diskriminante genügend große Faktoren der Form $2^i \cdot 3^j$. Da modulare Jacobische A_f höchstens modulo den Primteilern des Moduls N potentiell schlechte Reduktion haben können, berechnen wir die nun bessere ganzzahlige Annäherung von

$$\frac{\tilde{I}_{27}}{2^i \cdot 3^j} = \frac{i'_6 \cdot I_3^9}{2^i \cdot 3^j} =: \tilde{i_6}$$

für z.B. $i, j \in \{0, \ldots, 60\}$ und betrachten nur die $\tilde{i}_6$ mit $\lceil \tilde{i}_6 \rceil - \tilde{i}_6 < 10^{-b}$ bzw. $\lfloor \tilde{i}_6 \rfloor - \tilde{i}_6 < 10^{-b}$, so dass $\lceil \tilde{i}_6 \rceil$ bzw. $\lfloor \tilde{i}_6 \rfloor$ nur kleine Primfaktoren ($\leq N$) besitzen.
Im folgenden werden wir anhand eines Beispiels ausführlich die Funktionsweise unseres Algorithmus verdeutlichen.

Beispiel 5.2.5. Sei $N = 511 = 7 \cdot 73$ und f die Eigenform von $S_2^{\text{neu}}(511)$ mit der Fourier-Entwicklung

$$f \;=\; q + aq^2 + 2q^3 + (a^2-2)q^4 + (-a+1)q^5 + 2aq^6 + q^7 + (a-1)q^8 + q^9 + O(q^{10}),$$

wobei $a^3 - 5a + 1 = 0$. Die Abelsche Varietät A_f ist isomorph zu einem Torus, der eine symplektische Basis $\{\lambda_1, \ldots, \lambda_6\}$ besitzt, für die die Schnittpaarung H_f die Matrixdarstellung

$$(H_f(\lambda_i, \lambda_j))_{1 \leq i,j \leq 6} = \begin{pmatrix} 0 & \Delta_f \\ -\Delta_f & 0 \end{pmatrix} \in \mathbb{Z}^{6\times 6}$$

mit der Diagonalmatrix

$$\Delta_f = \begin{pmatrix} 2 & & \\ & 2 & \\ & & 2 \end{pmatrix}$$

annimmt. Nach Satz 5.2.2 ist A_f $\mathbb{Q}$-isogen zu einer prinzipal polarisierten Abelschen Varietät und besitzt die Torusdarstellung $\mathbb{C}^3/(\mathbb{Z}^3 + \Omega_f \mathbb{Z}^3)$ mit der Periodenmatrix

$$\Omega_f = \begin{pmatrix} -0.36441\cdots+0.77819\ldots i & -0.13786\cdots-0.04781\ldots i & -0.03929\cdots-0.20935\ldots i \\ -0.13786\cdots-0.04781\ldots i & -0.52538\cdots+0.94223\ldots i & -0.08244\cdots+0.64347\ldots i \\ -0.03929\cdots-0.20935\ldots i & -0.08244\cdots+0.64347\ldots i & 0.14824\cdots+1.15829\ldots i \end{pmatrix}.$$

Mit hoher Genauigkeit stellen wir fest, dass keine ihrer geraden Thetanullwerte verschwindet: Eine notwendige Bedingung dafür, dass A_f isomorph zur Jacobischen einer nicht-hyperelliptischen Kurve C_f vom Geschlecht 3 ist. Da $N = 511$ zusätzlich quadratfrei ist, ist A_f absolut einfach und somit isomorph zur Jacobischen einer nicht-hyperelliptischen Kurve C_f. Bezüglich des in 4.2 erwähnten kanonischen Aronhold-Systems $S = (\epsilon_i)$ berechnen wir mittels (4.1) die zu S assoziierten Bitangenten

$$\begin{aligned}
\beta_1: \quad 0 &= x - 1.46227\ldots y - 4.72415\ldots z \\
\beta_2: \quad 0 &= x + 0.96180\ldots y + 4.68326\ldots z \\
\beta_3: \quad 0 &= x - (0.20407\cdots-0.18026\ldots i)y - (0.06484\cdots-0.56249\ldots i)z \\
\beta_4: \quad 0 &= x + (0.57120\cdots-1.18552\ldots i)y + (0.90149\cdots-1.62543\ldots i)z \\
\beta_5: \quad 0 &= x + (2.52189\cdots+0.39416\ldots i)y - (3.17444\cdots+0.59506\ldots i)z \\
\beta_6: \quad 0 &= x - (0.40376\cdots+0.29179\ldots i)y + (0.09718\cdots-0.22804\ldots i)z \\
\beta_7: \quad 0 &= x + (0.34754\cdots+1.53705\ldots i)y + (1.79517\cdots+1.71851\ldots i)z
\end{aligned}$$

und nach linearen Transformationen erhalten wir

$$\begin{aligned}
\beta_1: \quad 0 &= x \\
\beta_2: \quad 0 &= y \\
\beta_3: \quad 0 &= z \\
\beta_4: \quad 0 &= x + y + z \\
\beta_5: \quad 0 &= x + (1.08745\cdots+0.04830\ldots i)y + (1.05224\cdots-0.03797\ldots i)z \\
\beta_6: \quad 0 &= x + (1.06127\cdots-0.03937\ldots i)y + (0.84409\cdots-0.01732\ldots i)z \\
\beta_7: \quad 0 &= x + (1.01087\cdots+0.04965\ldots i)y + (1.03160\cdots-0.09918\ldots i)z
\end{aligned}$$

Mittels Satz 4.2.2 berechnen wir das Riemann-Modell für die kanonische Einbettung der Kurve C_f

$$C_f: \ (xv_1 + yv_2 - zv_3)^2 = 4xyv_1v_2$$

mit

$$\begin{aligned}
v_1 &= (7.88335\cdots-10.5997\ldots i)x + (8.10793\cdots-11.2220\ldots i)y + (6.92042\cdots-11.3827\ldots i)z, \\
v_2 &= -(7.60169\cdots-6.77037\ldots i)x - (7.56578\cdots-7.03769\ldots i)y - (7.69385\cdots-7.38189\ldots i)z, \\
v_3 &= -(1.28165\cdots-3.82935\ldots i)x - (1.54215\cdots-4.18435\ldots i)y - (0.22657\cdots-4.00081\ldots i)z.
\end{aligned}$$

Die Kurve C_f besitzt die $\mathbb{Q}$-rationalen Dixmier-Invarianten

$$\begin{aligned}
i_1 &= 7.2252\ldots10^{-24} - 9.4189\ldots10^{-121}i &&= \tfrac{5^9\cdot37^9\cdot43133^9}{2^{53}\cdot3^{30}\cdot7^8\cdot11^{14}\cdot73^3\cdot101^{14}},\\
i_2 &= -1.2334\ldots10^{-24} + 1.5851\ldots10^{-121}i &&= \tfrac{-5^8\cdot37^7\cdot263\cdot43133^7\cdot197689\cdot6021091}{2^{57}\cdot3^{32}\cdot7^8\cdot11^{14}\cdot73^3\cdot101^{14}},\\
i_3 &= 6.2081\ldots10^{-18} - 8.8880\ldots10^{-112}i &&= \tfrac{5^6\cdot13\cdot37^6\cdot43133^6\cdot142702121\cdot25535098000501}{2^{43}\cdot3^{28}\cdot7^8\cdot11^{14}\cdot73^3\cdot101^{14}},\\
i_4 &= 2.4293\ldots10^{-16} + 4.6538\ldots10^{-111}i &&= \tfrac{5^5\cdot17\cdot37^5\cdot577\cdot43133^5\cdot3563719\cdot164875199\cdot160402791737}{2^{39}\cdot3^{28}\cdot7^8\cdot11^{14}\cdot73^3\cdot101^{14}},\\
i_5 &= -1.1873\ldots10^{-12} - 3.0158\ldots10^{-107}i &&= \tfrac{-5^4\cdot13^2\cdot37^4\cdot43133^4\cdot411537604667032828532884132805890 99}{2^{33}\cdot3^{24}\cdot7^8\cdot11^{14}\cdot73^3\cdot101^{14}},\\
i_6 &= -1.7786\ldots10^{-11} + 2.7155\ldots10^{-105}i &&= \tfrac{-5^3\cdot37^3\cdot43133^3\cdot688333\cdot28685999\cdot30314713933866742956065584376427 59}{2^{36}\cdot3^{26}\cdot7^8\cdot11^{14}\cdot73^3\cdot101^{14}}.
\end{aligned}$$

Für unsere nummerischen Berechnungen haben wir auf die Rechner vom Typ `Opteron` 246 (2GHz/ 8 GB Ram) des „Centre de calcul MEDICIS“

`http://medicis.polytechnique.fr`

zurückgegrifen.

Wir haben alle A_f mit $N \leq 4000$ bezüglich der kanonischen Polarisierung H_f untersucht. Von den 3334 Abelschen Varietäten A_f der Dimension 3 sind genau 79 bezüglich H_f prinzipal polarisiert. Darunter sind genau 12 der A_f hyperelliptisch:

$$X_{41}^A, X_{95}^A, X_{284}^B, X_{385}^F, X_{544}^I, X_{544}^J, X_{1136}^I, X_{1925}^V, X_{2600}^Y, X_{2624}^N, X_{2624}^O, X_{2695}^I$$

und 67 nicht-hyperelliptisch. Für die erhaltenen nicht-hyperelliptischen Kurven haben wir ihre Dixmier-Invarianten berechnet, und sie dann in Klassen von Kurven mit gleichen Invarianten unterteilt (siehe Tabelle 5.4). Obwohl es bis jetzt kein vollständiges Invariantensystem für glatte Quartiken gibt, vermuten wir, dass alle Kurven in den entsprechenden Klassen paarweise isomorph sind. Es gibt insgesamt 67 Kurven C_f vom Geschlecht 3 mit $\mathrm{Jac}(C_f) \simeq_{\mathbb{C}} A_f$, $f \in S_2^{\mathrm{neu}}(N)$ und $N \leq 4000$. Ist unsere Vermutung wahr, so gäbe es modulo Isomorphie nur 42 Kurven (s. Tabelle 5.4).

Die modularen Kurven C_i^j aus Tabelle 5.1 und Tabelle 5.2 besitzen die gleichen Dixmier-Invarianten wie die entsprechenden Kurven X_i^j aus Tabelle 5.4. Aus diesem Grund können wir auch annehmen, dass die Jacobischen $\mathrm{Jac}(C_i^j)$ und $\mathrm{Jac}(X_i^j)$ als unpolarisierte Abelsche Varietäten zur gleichen prinzipal polarisierten Isomorphieklasse gehören (siehe Abschnitt 4.1.3).

X^E_{187},	X^P_{2057},	X^S_{3179},	X^T_{3179}
X^F_{203},	X^N_{1421}		
X^A_{217},	X^C_{1519}		
X^A_{295},	X^C_{1475}		
X^C_{329},	X^G_{2303},		
X^D_{369},	X^E_{369}		
X^A_{388},	X^F_{1552}		
X^B_{436},	X^K_{1744}		
X^A_{452},	X^I_{1808}		
X^E_{475},	X^G_{475}		
X^B_{511},	X^E_{3577}		
X^H_{567},	X^Q_{3969}		
X^A_{596},	X^F_{2384}		
X^H_{656},	X^P_{2624},	X^S_{2624}	
X^B_{712},	X^H_{1424}		
X^H_{855},	X^J_{855}		
X^D_{1175},	X^E_{1175}		
X^H_{1308},	X^O_{3924}		
X^C_{1376},	X^D_{1376}		
X^G_{1900},	X^I_{1900}		
X^Q_{2432},	X^T_{2432}		
X^K_{3400},	X^Q_{3400}		

Tabelle 5.4: Klassifikation von nicht-hyperelliptischen Kurven mit $A_f \simeq \mathrm{Jac}(X)$ anhand ihrer Invarianten $i_1, \ldots, i_6$ ($g = 3$)

Kurve	Invarianten
X_{97}^A	$i_1 = \frac{-23^9}{2^{53}\cdot 3^{27}\cdot 97^3}$ $i_2 = \frac{5^2\cdot 23^7}{2^{57}\cdot 3^{29}\cdot 97^3}$ $i_3 = \frac{23^6\cdot 109}{2^{39}\cdot 3^{24}\cdot 97^3}$ $i_4 = \frac{-23^5\cdot 106649}{2^{37}\cdot 3^{25}\cdot 97^3}$ $i_5 = \frac{7\cdot 13\cdot 23^4\cdot 29\cdot 47}{2^{32}\cdot 3^{23}\cdot 97^3}$ $i_6 = \frac{7\cdot 23^3\cdot 4446899}{2^{29}\cdot 3^{22}\cdot 97^3}$
X_{109}^B	$i_1 = \frac{11^9}{2^{53}\cdot 3^{27}\cdot 109^3}$ $i_2 = \frac{11^7\cdot 47^2}{2^{57}\cdot 3^{29}\cdot 109^3}$ $i_3 = \frac{11^6\cdot 101\cdot 1259}{2^{43}\cdot 3^{24}\cdot 109^3}$ $i_4 = \frac{11^5\cdot 5894347}{2^{40}\cdot 3^{25}\cdot 109^3}$ $i_5 = \frac{11^5\cdot 5087\cdot 10889}{2^{37}\cdot 3^{23}\cdot 109^3}$ $i_6 = \frac{5\cdot 11^3\cdot 39330808093}{2^{36}\cdot 3^{22}\cdot 109^3}$
X_{113}^C	$i_1 = \frac{-1}{2^{53}\cdot 3^{27}\cdot 113^3}$ $i_2 = \frac{13\cdot 61}{2^{57}\cdot 3^{29}\cdot 113^3}$ $i_3 = \frac{-19\cdot 23\cdot 269}{2^{43}\cdot 3^{24}\cdot 113^3}$ $i_4 = \frac{-836063}{2^{39}\cdot 3^{25}\cdot 113^3}$ $i_5 = \frac{5\cdot 13\cdot 38562143}{2^{37}\cdot 3^{23}113^3}$ $i_6 = \frac{-11\cdot 37\cdot 62711911}{2^{36}\cdot 3^{22}\cdot 113^3}$
X_{127}^A	$i_1 = \frac{71^9}{2^{53}\cdot 3^{27}\cdot 127^3}$ $i_2 = \frac{-43\cdot 71^7\cdot 139}{2^{57}\cdot 3^{29}\cdot 127^3}$ $i_3 = \frac{7\cdot 71^6\cdot 13933}{2^{40}\cdot 3^{24}127^3}$ $i_4 = \frac{-7\cdot 71^5\cdot 23840251}{2^{41}\cdot 3^{25}\cdot 127^3}$ $i_5 = \frac{13\cdot 71^4\cdot 1336920521}{2^{38}3^{23}\cdot 127^3}$ $i_6 = \frac{53\cdot 71^3\cdot 607\cdot 3251\cdot 26681}{2^{36}\cdot 3^{22}\cdot 127^3}$
X_{139}^B	$i_1 = \frac{-17^9}{2^{53}\cdot 3^{27}\cdot 139^3}$ $i_2 = \frac{13\cdot 17^7\cdot 349}{2^{57}\cdot 3^{29}139^3}$ $i_3 = \frac{-7\cdot 17^6\cdot 41\cdot 367}{2^{43}\cdot 3^{24}\cdot 139^3}$ $i_4 = \frac{-7\cdot 17^5\cdot 2835667}{2^{40}\cdot 3^{25}\cdot 139^3}$ $i_5 = \frac{5\cdot 7\cdot 17^5\cdot 383\cdot 12161}{2^{34}\cdot 3^{23}\cdot 139^3}$ $i_6 = \frac{7\cdot 11\cdot 17^3\cdot 53\cdot 149854519}{2^{36}\cdot 3^{22}\cdot 139^3}$

Kurve	Invarianten
X^A_{149}	$i_1 = \frac{83^9}{2^{53}\cdot 3^{27}\cdot 149^3}$ $i_2 = \frac{83^7\cdot 1823}{2^{57}\cdot 3^{29}\cdot 149^3}$ $i_3 = \frac{5\cdot 83^6\cdot 239\cdot 947}{2^{41}\cdot 3^{24}\cdot 149^3}$ $i_4 = \frac{83^5\cdot 432110321}{2^{41}\cdot 3^{25}\cdot 149^3}$ $i_5 = \frac{7\cdot 83^4\cdot 236140337759}{2^{38}\cdot 3^{23}\cdot 149^3}$ $i_6 = \frac{5\cdot 7\cdot 17\cdot 23\cdot 83^3\cdot 239\cdot 853\cdot 58049}{2^{36}\cdot 3^{22}\cdot 149^3}$
X^A_{151}	$i_1 = \frac{7^9}{2^{53}\cdot 3^{27}\cdot 151^3}$ $i_2 = \frac{-7^7\cdot 17\cdot 617}{2^{57}\cdot 3^{29}\cdot 151^3}$ $i_3 = \frac{7^6\cdot 23\cdot 251\cdot 577}{2^{43}\cdot 3^{24}\cdot 151^3}$ $i_4 = \frac{7^5\cdot 11\cdot 1621\cdot 5087}{2^{40}\cdot 3^{25}\cdot 151^3}$ $i_5 = \frac{-7^4\cdot 31\cdot 37\cdot 113\cdot 587\cdot 6733}{2^{37}\cdot 3^{23}\cdot 151^3}$ $i_6 = \frac{7^3\cdot 38767\cdot 945648167}{2^{36}\cdot 3^{22}\cdot 151^3}$
X^B_{169}	$i_1 = \frac{5^{18}}{2^{53}\cdot 3^{27}\cdot 13^6}$ $i_2 = \frac{-5^{14}\cdot 7\cdot 79}{2^{57}\cdot 3^{29}\cdot 13^6}$ $i_3 = \frac{5^{12}\cdot 155887}{2^{43}\cdot 3^{24}\cdot 13^6}$ $i_4 = \frac{5^{10}\cdot 11\cdot 216829}{2^{39}\cdot 3^{25}\cdot 13^6}$ $i_5 = \frac{5^8\cdot 131\cdot 463\cdot 69847}{2^{37}\cdot 3^{23}\cdot 13^6}$ $i_6 = \frac{5^8\cdot 89\cdot 162518641}{2^{36}\cdot 3^{22}\cdot 13^6}$
X^B_{179}	$i_1 = \frac{-17^9}{2^{53}\cdot 3^{27}\cdot 179^3}$ $i_2 = \frac{17^8\cdot 89}{2^{57}\cdot 3^{29}\cdot 179^3}$ $i_3 = \frac{5^3\cdot 13\cdot 17^7}{2^{41}\cdot 3^{24}\cdot 179^3}$ $i_4 = \frac{-7\cdot 17^6\cdot 89\cdot 227}{2^{41}\cdot 3^{25}\cdot 179^3}$ $i_5 = \frac{17^5\cdot 41\cdot 2478937}{2^{38}\cdot 3^{23}\cdot 179^3}$ $i_6 = \frac{-17^3\cdot 36829407137}{2^{36}\cdot 3^{22}\cdot 179^3}$
X^E_{187}	$i_1 = \frac{7^9}{2^{44}\cdot 3^{27}\cdot 11^3\cdot 17^4}$ $i_2 = \frac{-7^7\cdot 59}{2^{48}\cdot 3^{29}\cdot 11^3\cdot 17^3}$ $i_3 = \frac{5\cdot 7^6\cdot 157\cdot 283}{2^{35}\cdot 3^{24}\cdot 11^3\cdot 17^4}$ $i_4 = \frac{-7^5\cdot 13\cdot 16456963}{2^{36}\cdot 3^{25}\cdot 11^3\cdot 17^4}$ $i_5 = \frac{7^4\cdot 111770067821}{2^{34}\cdot 3^{23}\cdot 11^3\cdot 17^4}$ $i_6 = \frac{-7^3\cdot 37\cdot 131\cdot 181\cdot 101419}{2^{32}\cdot 3^{22}\cdot 11^3\cdot 17^4}$

Kurve	Invarianten
X_{203}^F	$i_1 = \frac{7^4 \cdot 17^9}{2^{53} \cdot 3^{27} \cdot 29^3}$ $i_2 = \frac{5^3 \cdot 7^2 \cdot 17^7 \cdot 283}{2^{57} \cdot 3^{29} \cdot 29^3}$ $i_3 = \frac{5 \cdot 7 \cdot 17^6 \cdot 353 \cdot 29327}{2^{43} \cdot 3^{24} \cdot 29^3}$ $i_4 = \frac{7^2 \cdot 17^5 \cdot 487 \cdot 216577}{2^{40} \cdot 3^{25} \cdot 29^3}$ $i_5 = \frac{17^4 \cdot 6737 \cdot 8849 \cdot 359417}{2^{36} \cdot 3^{23} \cdot 7 \cdot 29^3}$ $i_6 = \frac{17^3 \cdot 149 \cdot 131679238350523}{2^{36} \cdot 3^{22} \cdot 7^2 \cdot 29^3}$
X_{217}^A	$i_1 = \frac{5^9 \cdot 227^9}{2^{53} \cdot 3^{55} \cdot 7^3 \cdot 31^3}$ $i_2 = \frac{-5^8 \cdot 227^7 \cdot 342821}{2^{57} \cdot 3^{57} \cdot 7^3 \cdot 31^3}$ $i_3 = \frac{5^6 \cdot 227^6 \cdot 439 \cdot 3871663}{2^{39} \cdot 3^{52} \cdot 7^3 \cdot 31^3}$ $i_4 = \frac{5^5 \cdot 19 \cdot 113 \cdot 227^5 \cdot 3181 \cdot 4410097}{2^{41} \cdot 3^{53} \cdot 7^3 \cdot 31^3}$ $i_5 = \frac{5^4 \cdot 227^4 \cdot 3264116968231423459}{2^{38} \cdot 3^{51} \cdot 7^3 \cdot 31^3}$ $i_6 = \frac{5^3 \cdot 227^3 \cdot 11320571 \cdot 514794731537767}{2^{36} \cdot 3^{50} \cdot 7^3 \cdot 31^3}$
X_{239}^A	$i_1 = \frac{5^9 \cdot 7^9}{2^{53} \cdot 3^{27} \cdot 239^3}$ $i_2 = \frac{-5^7 \cdot 7^7 \cdot 433}{2^{57} \cdot 3^{29} \cdot 239^3}$ $i_3 = \frac{-5^6 \cdot 7^6 \cdot 43963}{2^{39} \cdot 3^{24} \cdot 239^3}$ $i_4 = \frac{-5^5 \cdot 7^5 \cdot 509 \cdot 112481}{2^{41} \cdot 3^{25} \cdot 239^3}$ $i_5 = \frac{-5^4 \cdot 7^4 \cdot 27827 \cdot 3496799}{2^{38} \cdot 3^{23} \cdot 239^3}$ $i_6 = \frac{-5^4 \cdot 7^3 \cdot 68503144613}{2^{36} \cdot 3^{22} \cdot 239^3}$
X_{295}^A	$i_1 = \frac{-11^9}{2^{53} \cdot 3^{27} \cdot 5^3 \cdot 59^3}$ $i_2 = \frac{11^7 \cdot 13 \cdot 181}{2^{57} \cdot 3^{29} \cdot 5^3 \cdot 59^3}$ $i_3 = \frac{-7 \cdot 11^6 \cdot 23203}{2^{42} \cdot 3^{24} \cdot 5^3 \cdot 59^3}$ $i_4 = \frac{-7^2 \cdot 11^5 \cdot 370631}{2^{41} \cdot 3^{25} \cdot 5^3 \cdot 59^3}$ $i_5 = \frac{7 \cdot 11^5 \cdot 19 \cdot 769 \cdot 2287}{2^{38} \cdot 3^{23} \cdot 5^2 \cdot 59^3}$ $i_6 = \frac{-7 \cdot 11^3 \cdot 197 \cdot 415664659}{2^{36} \cdot 3^{22} \cdot 5^3 \cdot 59^3}$
X_{329}^C	$i_1 = \frac{-19^9}{2^{53} \cdot 3^{27} \cdot 7^3 \cdot 47^3}$ $i_2 = \frac{5 \cdot 19^7 \cdot 1181}{2^{57} \cdot 3^{29} \cdot 7^3 \cdot 47^3}$ $i_3 = \frac{-19^6 \cdot 29 \cdot 61 \cdot 67}{2^{40} \cdot 3^{24} \cdot 7^3 \cdot 47^3}$ $i_4 = \frac{-13 \cdot 19^5 \cdot 701 \cdot 7723}{2^{41} \cdot 3^{25} \cdot 7^3 \cdot 47^3}$ $i_5 = \frac{19^4 \cdot 163061001821}{2^{38} \cdot 3^{23} \cdot 7^3 \cdot 47^3}$ $i_6 = \frac{5 \cdot 19^3 \cdot 41 \cdot 7369 \cdot 904573}{2^{36} \cdot 3^{22} \cdot 7^3 \cdot 47^3}$

Kurve	Invarianten
X_{369}^{D}	$i_1 = \frac{7^9}{2^{44}\cdot 3^{18}\cdot 41^3}$ $i_2 = \frac{-7^7\cdot 97}{2^{48}\cdot 3^{21}\cdot 41^3}$ $i_3 = \frac{7^6\cdot 6353}{2^{36}\cdot 3^{16}\cdot 41^3}$ $i_4 = \frac{7^5\cdot 73\cdot 31337}{2^{36}\cdot 3^{18}\cdot 41^3}$ $i_5 = \frac{7^4\cdot 43\cdot 4662331}{2^{34}\cdot 3^{15}\cdot 41^3}$ $i_6 = \frac{-7^3\cdot 1307\cdot 1601\cdot 5303}{2^{32}\cdot 3^{16}\cdot 41^3}$
X_{369}^{E}	$i_1 = \frac{7^9}{2^{44}\cdot 3^{18}\cdot 41^3}$ $i_2 = \frac{-7^7\cdot 97}{2^{48}\cdot 3^{21}\cdot 41^3}$ $i_3 = \frac{7^6\cdot 6353}{2^{36}\cdot 3^{16}\cdot 41^3}$ $i_4 = \frac{7^5\cdot 73\cdot 31337}{2^{36}\cdot 3^{18}\cdot 41^3}$ $i_5 = \frac{7^4\cdot 43\cdot 4662331}{2^{34}\cdot 3^{15}\cdot 41^3}$ $i_6 = \frac{-7^3\cdot 1307\cdot 1601\cdot 5303}{2^{32}\cdot 3^{16}\cdot 41^3}$
X_{388}^{A}	$i_1 = \frac{-1}{2^{46}\cdot 3^{27}\cdot 97^3}$ $i_2 = \frac{-233}{2^{50}\cdot 3^{29}\cdot 97^3}$ $i_3 = \frac{5293513}{2^{41}\cdot 3^{24}\cdot 97^3}$ $i_4 = \frac{624203}{2^{35}\cdot 3^{25}\cdot 97^3}$ $i_5 = \frac{71\cdot 3533\cdot 300997}{2^{38}\cdot 3^{23}\cdot 97^3}$ $i_6 = \frac{-29\cdot 409326261863}{2^{36}\cdot 3^{22}\cdot 97^3}$
X_{436}^{B}	$i_1 = \frac{181^9}{2^{37}\cdot 3^{18}\cdot 11^{14}\cdot 109^3}$ $i_2 = \frac{-5\cdot 23\cdot 113\cdot 181^7}{2^{42}\cdot 3^{20}\cdot 11^{14}\cdot 109^3}$ $i_3 = \frac{181^6\cdot 4727066557}{2^{35}\cdot 3^{15}\cdot 11^{14}\cdot 109^3}$ $i_4 = \frac{181^5\cdot 499\cdot 56343733}{2^{33}\cdot 3^{15}\cdot 11^{14}\cdot 109^3}$ $i_5 = \frac{151\cdot 181^4\cdot 381481\cdot 538018951}{2^{34}\cdot 3^{14}\cdot 11^{14}\cdot 109^3}$ $i_6 = \frac{181^3\cdot 239273\cdot 480133\cdot 133676033}{2^{32}\cdot 3^{14}\cdot 11^{14}\cdot 109^3}$
X_{452}^{A}	$i_1 = \frac{31^9}{2^{10}\cdot 3^{41}\cdot 113^3}$ $i_2 = \frac{13\cdot 17\cdot 31^7\cdot 521}{2^{21}\cdot 3^{43}\cdot 113^3}$ $i_3 = \frac{31^6\cdot 157\cdot 336931631}{2^{17}\cdot 3^{38}\cdot 113^3}$ $i_4 = \frac{5\cdot 31^5\cdot 71\cdot 53551058051}{2^{18}\cdot 3^{39}\cdot 113^3}$ $i_5 = \frac{5\cdot 31^4\cdot 774401181277897891}{2^{22}\cdot 3^{37}\cdot 113^3}$ $i_6 = \frac{7\cdot 23\cdot 31^3\cdot 421\cdot 10301727084532427}{2^{22}\cdot 3^{36}\cdot 113^3}$

Kurve	Invarianten
X^E_{475}	$i_1 = \frac{3067^9}{2^{53}\cdot 3^{27}\cdot 5^6\cdot 19^3}$ $i_2 = \frac{479\cdot 3067^7\cdot 15937}{2^{57}\cdot 3^{29}\cdot 5^6\cdot 19^3}$ $i_3 = \frac{193\cdot 3067^6\cdot 115419877}{2^{39}\cdot 3^{24}\cdot 5^6\cdot 19^3}$ $i_4 = \frac{41\cdot 3067^5\cdot 41903\cdot 2234129}{2^{37}\cdot 3^{25}\cdot 5^4\cdot 19^3}$ $i_5 = \frac{13\cdot 397\cdot 479\cdot 3067^4\cdot 6619\cdot 8887\cdot 25349}{2^{32}\cdot 3^{23}\cdot 5^6\cdot 19^3}$ $i_6 = \frac{3067^3\cdot 1587899065951933060901}{2^{29}\cdot 3^{22}\cdot 5^5\cdot 19^3}$
X^G_{475}	$i_1 = \frac{3067^9}{2^{53}\cdot 3^{27}\cdot 5^6\cdot 19^3}$ $i_2 = \frac{479\cdot 3067^7\cdot 15937}{2^{57}\cdot 3^{29}\cdot 5^6\cdot 19^3}$ $i_3 = \frac{193\cdot 3067^6\cdot 115419877}{2^{39}\cdot 3^{24}\cdot 5^6\cdot 19^3}$ $i_4 = \frac{41\cdot 3067^5\cdot 41903\cdot 2234129}{2^{37}\cdot 3^{25}\cdot 5^4\cdot 19^3}$ $i_5 = \frac{13\cdot 397\cdot 479\cdot 3067^4\cdot 6619\cdot 8887\cdot 25349}{2^{32}\cdot 3^{23}\cdot 5^6\cdot 19^3}$ $i_6 = \frac{3067^3\cdot 1587899065951933060901}{2^{29}\cdot 3^{22}\cdot 5^5\cdot 19^3}$
X^B_{511}	$i_1 = \frac{5^9\cdot 37^9\cdot 43133^9}{2^{53}\cdot 3^{30}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}$ $i_2 = \frac{-5^8\cdot 37^7\cdot 263\cdot 43133^7\cdot 197689\cdot 6021091}{2^{57}\cdot 3^{32}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}$ $i_3 = \frac{5^6\cdot 13\cdot 37^6\cdot 43133^6\cdot 142702121\cdot 25535098000501}{2^{43}\cdot 3^{28}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}$ $i_4 = \frac{5^5\cdot 17\cdot 37^5\cdot 577\cdot 43133^5\cdot 3563719\cdot 164875199\cdot 160402791737}{2^{39}\cdot 3^{28}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}$ $i_5 = \frac{-5^4\cdot 13^2\cdot 37^4\cdot 43133^4\cdot 4115376046670328285328841328058 0099}{2^{33}\cdot 3^{24}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}$ $i_6 = \frac{-5^3\cdot 37^3\cdot 43133^3\cdot 688333\cdot 28685999\cdot 3031471393386674295606558437642759}{2^{36}\cdot 3^{26}\cdot 7^8\cdot 11^{14}\cdot 73^3\cdot 101^{14}}$
X^H_{567}	$i_1 = \frac{5^4}{2^{53}\cdot 3^9\cdot 7^3}$ $i_2 = \frac{5\cdot 17}{2^{57}\cdot 3^{12}\cdot 7^3}$ $i_3 = \frac{5\cdot 3821}{2^{42}\cdot 3^8\cdot 7^3}$ $i_4 = \frac{17\cdot 8363}{2^{41}\cdot 3^9\cdot 5\cdot 7^3}$ $i_5 = \frac{5^2\cdot 313}{2^{38}\cdot 3^6\cdot 7^3}$ $i_6 = \frac{-19\cdot 83\cdot 11119}{2^{36}\cdot 3^7\cdot 5^2\cdot 7^3}$
X^A_{596}	$i_1 = \frac{359^9}{2^{55}\cdot 3^{27}\cdot 149^3}$ $i_2 = \frac{13\cdot 23\cdot 73\cdot 359^7}{2^{57}\cdot 3^{29}\cdot 149^3}$ $i_3 = \frac{23\cdot 359^6\cdot 89348191}{2^{47}\cdot 3^{24}\cdot 149^3}$ $i_4 = \frac{5^2\cdot 359^5\cdot 39644905697}{2^{45}\cdot 3^{25}\cdot 149^3}$ $i_5 = \frac{47\cdot 359^4\cdot 370708577229919}{2^{42}\cdot 3^{23}\cdot 149^3}$ $i_6 = \frac{13\cdot 19\cdot 359^3\cdot 16529\cdot 794641\cdot 2599117}{2^{40}\cdot 3^{22}\cdot 149^3}$

Kurve	Invarianten
X^I_{637}	$i_1 = \frac{5^9 \cdot 53^9}{2^{44} \cdot 3^{41} \cdot 7^7 \cdot 13^5}$ $i_2 = \frac{5^7 \cdot 53^7 \cdot 103 \cdot 6287}{2^{48} \cdot 3^{43} \cdot 7^7 \cdot 13^5}$ $i_3 = \frac{-5^7 \cdot 17 \cdot 53^6 \cdot 854383}{2^{37} \cdot 3^{38} \cdot 7^5 \cdot 13^5}$ $i_4 = \frac{-5^5 \cdot 53^5 \cdot 3319 \cdot 2226319}{2^{36} \cdot 3^{39} \cdot 7^4 \cdot 13^5}$ $i_5 = \frac{-5^4 \cdot 19 \cdot 53^4 \cdot 83 \cdot 150270627149}{2^{34} \cdot 3^{37} \cdot 7^4 \cdot 13^5}$ $i_6 = \frac{5^4 \cdot 17 \cdot 53^3 \cdot 67 \cdot 101 \cdot 25928164139}{2^{32} \cdot 3^{36} \cdot 7^3 \cdot 13^5}$
X^H_{656}	$i_1 = \frac{-3733^9}{2^{105} \cdot 3^{27} \cdot 41^3}$ $i_2 = \frac{-5 \cdot 3733^7 \cdot 406177}{2^{107} \cdot 3^{29} \cdot 41^3}$ $i_3 = \frac{-7 \cdot 149 \cdot 3733^6 \cdot 16879 \cdot 167393}{2^{97} \cdot 3^{24} \cdot 41^3}$ $i_4 = \frac{-5^3 \cdot 103 \cdot 199 \cdot 743 \cdot 3733^5 \cdot 8299073}{2^{95} \cdot 3^{25} \cdot 41^3}$ $i_5 = \frac{-3733^4 \cdot 405401 \cdot 27712897 \cdot 133880407}{2^{91} \cdot 3^{23} \cdot 41^3}$ $i_6 = \frac{-5 \cdot 1999 \cdot 3733^3 \cdot 443533 \cdot 46191865920463}{2^{89} \cdot 3^{22} \cdot 41^2}$
X^B_{712}	$i_1 = \frac{7^9 \cdot 17^9 \cdot 293^9}{2^{50} \cdot 3^{27} \cdot 11^{14} \cdot 47^{14} \cdot 89^3}$ $i_2 = \frac{-7^7 \cdot 13 \cdot 17^7 \cdot 293^7 \cdot 69188363}{2^{47} \cdot 3^{29} \cdot 11^{14} \cdot 47^{14} \cdot 89^3}$ $i_3 = \frac{-7^6 \cdot 17^6 \cdot 131 \cdot 293^6 \cdot 1566637 \cdot 4274128217}{2^{45} \cdot 3^{24} \cdot 11^{14} \cdot 47^{14} \cdot 89^3}$ $i_4 = \frac{-5 \cdot 7^5 \cdot 17^5 \cdot 293^5 \cdot 18553 \cdot 1577539 \cdot 228276891527}{2^{42} \cdot 3^{25} \cdot 11^{14} \cdot 47^{14} \cdot 89^3}$ $i_5 = \frac{5 \cdot 7^4 \cdot 17^4 \cdot 293^4 \cdot 167708407 \cdot 5945094836922119845873}{2^{40} \cdot 3^{23} \cdot 11^{14} \cdot 47^{14} \cdot 89^3}$ $i_6 = \frac{-7^3 \cdot 17^3 \cdot 293^3 \cdot 1074361 \cdot 4594141567 \cdot 5718478988993520877}{2^{35} \cdot 3^{22} \cdot 11^{14} \cdot 47^{14} \cdot 89^3}$
X^B_{776}	$i_1 = \frac{-5^9 \cdot 281^9}{2^{28} \cdot 3^9 \cdot 97^3 \cdot 277^{14}}$ $i_2 = \frac{-5^7 \cdot 7107 \cdot 163 \cdot 281^7 \cdot 3583}{2^{36} \cdot 3^{12} \cdot 97^3 \cdot 277^{14}}$ $i_3 = \frac{5^6 \cdot 233 \cdot 281^6 \cdot 5501 \cdot 1708780933}{2^{29} \cdot 3^{10} \cdot 97^3 \cdot 277^{14}}$ $i_4 = \frac{-5^5 \cdot 7 \cdot 281^5 \cdot 206942796061260631}{2^{28} \cdot 3^{11} \cdot 97^3 \cdot 277^{14}}$ $i_5 = \frac{5^5 \cdot 43 \cdot 281^4 \cdot 693757 \cdot 227889956800771}{2^{30} \cdot 3^8 \cdot 97^3 \cdot 277^{14}}$ $i_6 = \frac{5^3 \cdot 7 \cdot 281^3 \cdot 983058785167777931502530 1731}{2^{29} \cdot 3^{10} \cdot 97^3 \cdot 277^{14}}$
X^H_{855}	$i_1 = \frac{1}{2^{53} \cdot 3^{18} \cdot 5^3 \cdot 19^4}$ $i_2 = \frac{-419}{2^{57} \cdot 3^{21} \cdot 5^3 \cdot 19^4}$ $i_3 = \frac{-23 \cdot 53}{2^{43} \cdot 3^{16} \cdot 5^3 \cdot 19^4}$ $i_4 = \frac{-11551}{2^{39} \cdot 3^{18} \cdot 5^3 \cdot 19^4}$ $i_5 = \frac{97 \cdot 1459}{2^{36} \cdot 3^{15} \cdot 5^2 \cdot 19^4}$ $i_6 = \frac{11 \cdot 23 \cdot 41 \cdot 15773}{2^{36} \cdot 3^{15} \cdot 5^3 \cdot 19^4}$

Kurve	Invarianten
X^K_{855}	$i_1 = \frac{1}{2^{53}\cdot 3^{18}\cdot 5^3\cdot 19^4}$ $i_2 = \frac{-419}{2^{57}\cdot 3^{21}\cdot 5^3\cdot 19^4}$ $i_3 = \frac{-23\cdot 53}{2^{43}\cdot 3^{16}\cdot 5^3\cdot 19^4}$ $i_4 = \frac{-11551}{2^{39}\cdot 3^{18}\cdot 5^3\cdot 19^4}$ $i_5 = \frac{97\cdot 1459}{2^{36}\cdot 3^{15}\cdot 5^2\cdot 19^4}$ $i_6 = \frac{11\cdot 23\cdot 41\cdot 15773}{2^{36}\cdot 3^{15}\cdot 5^3\cdot 19^4}$
X^D_{1175}	$i_1 = \frac{29^9}{2^{53}\cdot 3^{27}\cdot 5^6\cdot 47^3}$ $i_2 = \frac{-7\cdot 29^7\cdot 79}{2^{57}\cdot 3^{29}\cdot 5^6\cdot 47^3}$ $i_3 = \frac{29^6\cdot 47119}{2^{38}\cdot 3^{24}\cdot 5^6\cdot 47^3}$ $i_4 = \frac{11\cdot 29^5\cdot 138661}{2^{41}\cdot 3^{25}\cdot 5^4\cdot 47^3}$ $i_5 = \frac{13\cdot 29^4\cdot 449\cdot 2791\cdot 3221}{2^{37}\cdot 3^{23}\cdot 5^6\cdot 47^3}$ $i_6 = \frac{29^3\cdot 37\cdot 43\cdot 233\cdot 653\cdot 6823}{2^{36}\cdot 3^{22}\cdot 5^5\cdot 47^3}$
X^E_{1175}	$i_1 = \frac{29^9}{2^{53}\cdot 3^{27}\cdot 5^6\cdot 47^3}$ $i_2 = \frac{-7\cdot 29^7\cdot 79}{2^{57}\cdot 3^{29}\cdot 5^6\cdot 47^3}$ $i_3 = \frac{29^6\cdot 47119}{2^{38}\cdot 3^{24}\cdot 5^6\cdot 47^3}$ $i_4 = \frac{11\cdot 29^5\cdot 138661}{2^{41}\cdot 3^{25}\cdot 5^4\cdot 47^3}$ $i_5 = \frac{13\cdot 29^4\cdot 449\cdot 2791\cdot 3221}{2^{37}\cdot 3^{23}\cdot 5^6\cdot 47^3}$ $i_6 = \frac{29^3\cdot 37\cdot 43\cdot 233\cdot 653\cdot 6823}{2^{36}\cdot 3^{22}\cdot 5^5\cdot 47^3}$
X^P_{1215}	$i_1 = \frac{-1}{2^{53}\cdot 3^{15}\cdot 5^9}$ $i_2 = \frac{-7}{2^{57}\cdot 3^{17}\cdot 5^9}$ $i_3 = \frac{-431}{2^{42}\cdot 3^{12}\cdot 5^9}$ $i_4 = \frac{6571}{2^{41}\cdot 3^{13}\cdot 5^9}$ $i_5 = \frac{563}{2^{32}\cdot 3^{10}\cdot 5^8}$ $i_6 = \frac{-71\cdot 155723}{2^{36}\cdot 3^{11}\cdot 5^9}$
X^H_{1308}	$i_1 = \frac{7^9\cdot 167^9}{2^{37}\cdot 3^{42}\cdot 5^{12}\cdot 109^3}$ $i_2 = \frac{-7^8\cdot 103\cdot 167^7\cdot 2287}{2^{41}\cdot 3^{44}\cdot 5^{12}\cdot 109^3}$ $i_3 = \frac{7^7\cdot 11\cdot 167^6\cdot 3971210053}{2^{35}\cdot 3^{39}\cdot 5^{12}\cdot 109^3}$ $i_4 = \frac{-7^5\cdot 113\cdot 167^5\cdot 787\cdot 17657\cdot 52301}{2^{33}\cdot 3^{40}\cdot 5^{11}\cdot 109^3}$ $i_5 = \frac{7^4\cdot 163\cdot 167^4\cdot 68819\cdot 1639520011631}{2^{32}\cdot 3^{38}\cdot 5^{11}\cdot 109^3}$ $i_6 = \frac{7^3\cdot 11\cdot 167^3\cdot 307\cdot 65484401\cdot 1299470603113}{2^{31}\cdot 3^{37}\cdot 5^{12}\cdot 109^3}$

Kurve	Invarianten
X^C_{1376}	$i_1 = \frac{-179^9}{2^{65}\cdot 3^{27}\cdot 43^3}$ $i_2 = \frac{179^7\cdot 1447}{2^{67}\cdot 3^{29}\cdot 43^3}$ $i_3 = \frac{-37\cdot 179^6\cdot 227\cdot 7237}{2^{57}\cdot 3^{24}\cdot 43^3}$ $i_4 = \frac{179^5\cdot 257\cdot 3389\cdot 4861}{2^{55}\cdot 3^{25}\cdot 43^3}$ $i_5 = \frac{127\cdot 179^4\cdot 773\cdot 59559133}{2^{51}\cdot 3^{23}\cdot 43^3}$ $i_6 = \frac{179^3\cdot 24851\cdot 34961\cdot 667697}{2^{49}\cdot 3^{22}\cdot 43^3}$
X^D_{1376}	$i_1 = \frac{-179^9}{2^{65}\cdot 3^{27}\cdot 43^3}$ $i_2 = \frac{179^7\cdot 1447}{2^{67}\cdot 3^{29}\cdot 43^3}$ $i_3 = \frac{-37\cdot 179^6\cdot 227\cdot 7237}{2^{57}\cdot 3^{24}\cdot 43^3}$ $i_4 = \frac{179^5\cdot 257\cdot 3389\cdot 4861}{2^{55}\cdot 3^{25}\cdot 43^3}$ $i_5 = \frac{127\cdot 179^4\cdot 773\cdot 59559133}{2^{51}\cdot 3^{23}\cdot 43^3}$ $i_6 = \frac{179^3\cdot 24851\cdot 34961\cdot 667697}{2^{49}\cdot 3^{22}\cdot 43^3}$
X^N_{1421}	$i_1 = \frac{7^4\cdot 17^9}{2^{53}\cdot 3^{27}\cdot 29^3}$ $i_2 = \frac{5^3\cdot 7^2\cdot 17^7\cdot 283}{2^{57}\cdot 3^{29}\cdot 29^3}$ $i_3 = \frac{5\cdot 7\cdot 17^6\cdot 353\cdot 29327}{2^{43}\cdot 3^{24}\cdot 29^3}$ $i_4 = \frac{7^2\cdot 17^5\cdot 487\cdot 216577}{2^{40}\cdot 3^{25}\cdot 29^3}$ $i_5 = \frac{17^4\cdot 6737\cdot 8849\cdot 359417}{2^{36}\cdot 3^{23}\cdot 7\cdot 29^3}$ $i_6 = \frac{17^3\cdot 149\cdot 131679238350523}{2^{36}\cdot 3^{22}\cdot 7^2\cdot 29^3}$
X^H_{1424}	$i_1 = \frac{7^9\cdot 17^9\cdot 293^9}{2^{50}\cdot 3^{27}\cdot 11^{14}\cdot 47^{14}\cdot 89^3}$ $i_2 = \frac{-7^7\cdot 13\cdot 17^7\cdot 293^7\cdot 69188363}{2^{47}\cdot 3^{29}\cdot 11^{14}\cdot 47^{14}\cdot 89^3}$ $i_3 = \frac{-7^6\cdot 17^6\cdot 131\cdot 293^6\cdot 1566637\cdot 4274128217}{2^{45}\cdot 3^{24}\cdot 11^{14}\cdot 47^{14}\cdot 89^3}$ $i_4 = \frac{-5\cdot 7^5\cdot 17^5\cdot 293^5\cdot 18553\cdot 1577539\cdot 228276891527}{2^{42}\cdot 3^{25}\cdot 11^{14}\cdot 47^{14}\cdot 89^3}$ $i_5 = \frac{5\cdot 7^4\cdot 17^4\cdot 293^4\cdot 167708407\cdot 5945094836922119845873}{2^{40}\cdot 3^{23}\cdot 11^{14}\cdot 47^{14}\cdot 89^3}$ $i_6 = \frac{-7^3\cdot 17^3\cdot 293^3\cdot 1074361\cdot 4594141567\cdot 5718478988993520877}{2^{35}\cdot 3^{22}\cdot 11^{14}\cdot 47^{14}\cdot 89^3}$
X^C_{1475}	$i_1 = \frac{-11^9}{2^{53}\cdot 3^{27}\cdot 5^3\cdot 59^3}$ $i_2 = \frac{11^7\cdot 13\cdot 181}{2^{57}\cdot 3^{29}\cdot 5^3\cdot 59^3}$ $i_3 = \frac{-7\cdot 11^6\cdot 23203}{2^{42}\cdot 3^{24}\cdot 5^3\cdot 59^3}$ $i_4 = \frac{-7^2\cdot 11^5\cdot 370631}{2^{41}\cdot 3^{25}\cdot 5^3\cdot 59^3}$ $i_5 = \frac{7\cdot 11^5\cdot 19\cdot 769\cdot 2287}{2^{38}\cdot 3^{23}\cdot 5^2\cdot 59^3}$ $i_6 = \frac{-7\cdot 11^3\cdot 197\cdot 415664659}{2^{36}\cdot 3^{22}\cdot 5^3\cdot 59^3}$

Kurve	Invarianten
X^C_{1519}	$i_1 = \frac{5^9 \cdot 227^9}{2^{53} \cdot 3^{55} \cdot 7^3 \cdot 31^3}$ $i_2 = \frac{-5^8 \cdot 227^7 \cdot 342821}{2^{57} \cdot 3^{57} \cdot 7^3 \cdot 31^3}$ $i_3 = \frac{5^6 \cdot 227^6 \cdot 439 \cdot 3871663}{2^{39} \cdot 3^{52} \cdot 7^3 \cdot 31^3}$ $i_4 = \frac{5^5 \cdot 19 \cdot 113 \cdot 227^5 \cdot 3181 \cdot 4410097}{2^{41} \cdot 3^{53} \cdot 7^3 \cdot 31^3}$ $i_5 = \frac{5^4 \cdot 227^4 \cdot 3264116968231423459}{2^{38} \cdot 3^{51} \cdot 7^3 \cdot 31^3}$ $i_6 = \frac{5^3 \cdot 227^3 \cdot 11320571 \cdot 514794731537767}{2^{36} \cdot 3^{50} \cdot 7^3 \cdot 31^3}$
X^C_{1552}	$i_1 = \frac{-5^9 \cdot 281^9}{2^{28} \cdot 3^9 \cdot 97^3 \cdot 277^{14}}$ $i_2 = \frac{5^7 \cdot 7 \cdot 107 \cdot 163 \cdot 281^7 \cdot 3583}{2^{36} \cdot 3^{12} \cdot 97^3 \cdot 277^{14}}$ $i_3 = \frac{5^6 \cdot 233 \cdot 281^6 \cdot 5501 \cdot 1708780933}{2^{29} \cdot 3^{10} \cdot 97^3 \cdot 277^{14}}$ $i_4 = \frac{-5^5 \cdot 7 \cdot 281^5 \cdot 206942796061260631}{2^{28} \cdot 3^{11} \cdot 97^3 \cdot 277^{14}}$ $i_5 = \frac{5^5 \cdot 43 \cdot 281^4 \cdot 693757 \cdot 227889956800771}{2^{30} \cdot 3^8 \cdot 97^3 \cdot 277^{14}}$ $i_6 = \frac{-5^3 \cdot 7 \cdot 281^3 \cdot 98305878516777793150253017 31}{2^{29} \cdot 3^{10} \cdot 97^3 \cdot 277^{14}}$
X^F_{1552}	$i_1 = \frac{-1}{2^{46} \cdot 3^{27} \cdot 97^3}$ $i_2 = \frac{-233}{2^{50} \cdot 3^{29} \cdot 97^3}$ $i_3 = \frac{5293513}{2^{41} \cdot 3^{24} \cdot 97^3}$ $i_4 = \frac{624203}{2^{35} \cdot 3^{25} \cdot 97^3}$ $i_5 = \frac{71 \cdot 3533 \cdot 300997}{2^{38} \cdot 3^{23} \cdot 97^3}$ $i_6 = \frac{-29 \cdot 409326261863}{2^{36} \cdot 3^{22} \cdot 97^3}$
X^B_{1681}	$i_1 = \frac{-101^9}{2^{53} \cdot 3^{27} \cdot 41^6}$ $i_2 = \frac{5^2 \cdot 7 \cdot 101^7 \cdot 127}{2^{57} \cdot 3^{29} \cdot 41^6}$ $i_3 = \frac{23 \cdot 97 \cdot 101^6 \cdot 727}{2^{42} \cdot 3^{24} \cdot 41^6}$ $i_4 = \frac{-101^5 \cdot 661 \cdot 413579}{2^{41} \cdot 3^{25} \cdot 41^6}$ $i_5 = \frac{101^4 \cdot 1549 \cdot 384738751}{2^{38} \cdot 3^{23} \cdot 41^6}$ $i_6 = \frac{-5^2 \cdot 101^3 \cdot 1931 \cdot 15739 \cdot 86689}{2^{36} \cdot 3^{22} \cdot 41^6}$
X^K_{1744}	$i_1 = \frac{181^9}{2^{37} \cdot 3^{18} \cdot 11^{14} \cdot 109^3}$ $i_2 = \frac{-5 \cdot 23 \cdot 113 \cdot 181^7}{2^{42} \cdot 3^{20} \cdot 11^{14} \cdot 109^3}$ $i_3 = \frac{181^6 \cdot 4727066557}{2^{35} \cdot 3^{15} \cdot 11^{14} \cdot 109^3}$ $i_4 = \frac{181^5 \cdot 499 \cdot 56343733}{2^{33} \cdot 3^{15} \cdot 11^{14} \cdot 109^3}$ $i_5 = \frac{151 \cdot 181^4 \cdot 381481 \cdot 538018951}{2^{34} \cdot 3^{14} \cdot 11^{14} \cdot 109^3}$ $i_6 = \frac{181^3 \cdot 239273 \cdot 480133 \cdot 133676033}{2^{32} \cdot 3^{14} \cdot 11^{14} \cdot 109^3}$

Kurve	Invarianten
X^I_{1808}	$i_1 = \frac{31^9}{2^{10}\cdot 3^{41}\cdot 113^3}$ $i_2 = \frac{13\cdot 17\cdot 31^7\cdot 521}{2^{21}\cdot 3^{43}\cdot 113^3}$ $i_3 = \frac{31^6\cdot 157\cdot 336931631}{2^{17}\cdot 3^{38}\cdot 113^3}$ $i_4 = \frac{5\cdot 31^5\cdot 71\cdot 53551058051}{2^{18}\cdot 3^{39}\cdot 113^3}$ $i_5 = \frac{5\cdot 31^4\cdot 774401181277897891}{2^{22}\cdot 3^{37}\cdot 113^3}$ $i_6 = \frac{7\cdot 23\cdot 31^3\cdot 421\cdot 10301727084532427}{2^{22}\cdot 3^{36}\cdot 113^3}$
X^G_{1900}	$i_1 = \frac{5881^9}{2^{46}\cdot 3^{27}\cdot 5^2\cdot 19^3\cdot 37^{14}}$ $i_2 = \frac{11\cdot 5881^7\cdot 34719863}{2^{50}\cdot 3^{29}\cdot 5^3\cdot 19^3\cdot 37^{14}}$ $i_3 = \frac{941\cdot 1753\cdot 5881^6\cdot 5267096059}{2^{41}\cdot 3^{24}\cdot 5^4\cdot 19^3\cdot 37^{14}}$ $i_4 = \frac{13\cdot 227\cdot 463\cdot 1579\cdot 5881^5\cdot 7617975877}{2^{36}\cdot 3^{25}\cdot 5^4\cdot 19^3\cdot 37^{14}}$ $i_5 = \frac{571\cdot 5881^4\cdot 1817952414429245682273271}{2^{38}\cdot 3^{23}\cdot 5^5\cdot 19^3\cdot 37^{14}}$ $i_6 = \frac{11^2\cdot 5881^3\cdot 7274639\cdot 1112884133665941938690 57}{2^{36}\cdot 3^{22}\cdot 5^6\cdot 19^3\cdot 37^{14}}$
X^I_{1900}	$i_1 = \frac{5881^9}{2^{46}\cdot 3^{27}\cdot 5^2\cdot 19^3\cdot 37^{14}}$ $i_2 = \frac{11\cdot 5881^7\cdot 34719863}{2^{50}\cdot 3^{29}\cdot 5^3\cdot 19^3\cdot 37^{14}}$ $i_3 = \frac{941\cdot 1753\cdot 5881^6\cdot 5267096059}{2^{41}\cdot 3^{24}\cdot 5^4\cdot 19^3\cdot 37^{14}}$ $i_4 = \frac{13\cdot 227\cdot 463\cdot 1579\cdot 5881^5\cdot 7617975877}{2^{36}\cdot 3^{25}\cdot 5^4\cdot 19^3\cdot 37^{14}}$ $i_5 = \frac{571\cdot 5881^4\cdot 1817952414429245682273271}{2^{38}\cdot 3^{23}\cdot 5^5\cdot 19^3\cdot 37^{14}}$ $i_6 = \frac{11^2\cdot 5881^3\cdot 7274639\cdot 1112884133665941938690 57}{2^{36}\cdot 3^{22}\cdot 5^6\cdot 19^3\cdot 37^{14}}$
X^P_{2057}	$i_1 = \frac{7^9}{2^{44}\cdot 3^{27}\cdot 11^3\cdot 17^4}$ $i_2 = \frac{-7^7\cdot 59}{2^{48}\cdot 3^{29}\cdot 11^3\cdot 17^3}$ $i_3 = \frac{5\cdot 7^6\cdot 157\cdot 283}{2^{35}\cdot 3^{24}\cdot 11^3\cdot 17^4}$ $i_4 = \frac{-7^5\cdot 13\cdot 16456963}{2^{36}\cdot 3^{25}\cdot 11^3\cdot 17^4}$ $i_5 = \frac{7^4\cdot 111770067821}{2^{34}\cdot 3^{23}\cdot 11^3\cdot 17^4}$ $i_6 = \frac{-7^3\cdot 37\cdot 131\cdot 181\cdot 101419}{2^{32}\cdot 3^{22}\cdot 11^3\cdot 17^4}$
X^G_{2303}	$i_1 = \frac{-19^9}{2^{53}\cdot 3^{27}\cdot 7^3\cdot 47^3}$ $i_2 = \frac{5\cdot 19^7\cdot 1181}{2^{57}\cdot 3^{29}\cdot 7^3\cdot 47^3}$ $i_3 = \frac{-19^6\cdot 29\cdot 61\cdot 67}{2^{40}\cdot 3^{24}\cdot 7^3\cdot 47^3}$ $i_4 = \frac{-13\cdot 19^5\cdot 701\cdot 7723}{2^{41}\cdot 3^{25}\cdot 7^3\cdot 47^3}$ $i_5 = \frac{19^4\cdot 163061001821}{2^{38}\cdot 3^{23}\cdot 7^3\cdot 47^3}$ $i_6 = \frac{5\cdot 19^3\cdot 41\cdot 7369\cdot 904573}{2^{36}\cdot 3^{22}\cdot 7^3\cdot 47^3}$

Kurve	Invarianten
X^D_{2332}	$i_1 = \frac{-89^9 \cdot 25633^9}{2^{45} \cdot 3^{27} \cdot 11^4 \cdot 17^{28} \cdot 53^4}$ $i_2 = \frac{7 \cdot 89^7 \cdot 5107 \cdot 25633^7 \cdot 41317517}{2^{50} \cdot 3^{29} \cdot 11^4 \cdot 17^{28} \cdot 53^4}$ $i_3 = \frac{-89^6 \cdot 2857 \cdot 25633^6 \cdot 2148527 \cdot 3056961798049}{2^{43} \cdot 3^{24} \cdot 11^4 \cdot 17^{28} \cdot 53^4}$ $i_4 = \frac{-89^5 \cdot 1033 \cdot 25633^5 \cdot 1928593721 \cdot 469821080308193}{2^{36} \cdot 3^{25} \cdot 11^4 \cdot 17^{28} \cdot 53^4}$ $i_5 = \frac{-89^4 \cdot 127 \cdot 167 \cdot 1013 \cdot 4241 \cdot 25633^4 \cdot 135719 \cdot 105716509 \cdot 48398472322229}{2^{42} \cdot 3^{23} \cdot 11^4 \cdot 17^{28} \cdot 53^4}$ $i_6 = \frac{-5 \cdot 89^3 \cdot 491 \cdot 1481 \cdot 25633^3 \cdot 77979497 \cdot 5481540718285374915636977355 17}{2^{40} \cdot 3^{22} \cdot 11^4 \cdot 17^{28} \cdot 53^4}$
X^F_{2384}	$i_1 = \frac{359^9}{2^{55} \cdot 3^{27} \cdot 149^3}$ $i_2 = \frac{13 \cdot 23 \cdot 73 \cdot 359^7}{2^{57} \cdot 3^{29} \cdot 149^3}$ $i_3 = \frac{23 \cdot 359^6 \cdot 89348191}{2^{47} \cdot 3^{24} \cdot 149^3}$ $i_4 = \frac{5^2 \cdot 359^5 \cdot 39644905697}{2^{45} \cdot 3^{25} \cdot 149^3}$ $i_5 = \frac{47 \cdot 359^4 \cdot 370708577229919}{2^{42} \cdot 3^{23} \cdot 149^3}$ $i_6 = \frac{13 \cdot 19 \cdot 359^3 \cdot 16529 \cdot 794641 \cdot 2599117}{2^{40} \cdot 3^{22} \cdot 149^3}$
X^Q_{2432}	$i_1 = \frac{7^9 \cdot 353^9}{2^{67} \cdot 3^{41} \cdot 19^3}$ $i_2 = \frac{7^7 \cdot 353^7 \cdot 343193}{2^{69} \cdot 3^{43} \cdot 19^3}$ $i_3 = \frac{7^6 \cdot 13 \cdot 353^6 \cdot 1091221199}{2^{59} \cdot 3^{38} \cdot 19^2}$ $i_4 = \frac{7^5 \cdot 353^5 \cdot 8897857 \cdot 47113439}{2^{57} \cdot 3^{39} \cdot 19^3}$ $i_5 = \frac{5^2 \cdot 7^4 \cdot 53 \cdot 61 \cdot 353^4 \cdot 1414211 \cdot 162129559}{2^{53} \cdot 3^{37} \cdot 19^3}$ $i_6 = \frac{5 \cdot 7^3 \cdot 17 \cdot 131 \cdot 353^3 \cdot 6821753 \cdot 579475796821}{2^{51} \cdot 3^{36} \cdot 19^3}$
X^T_{2432}	$i_1 = \frac{7^9 \cdot 353^9}{2^{67} \cdot 3^{41} \cdot 19^3}$ $i_2 = \frac{7^7 \cdot 353^7 \cdot 343193}{2^{69} \cdot 3^{43} \cdot 19^3}$ $i_3 = \frac{7^6 \cdot 13 \cdot 353^6 \cdot 1091221199}{2^{59} \cdot 3^{38} \cdot 19^2}$ $i_4 = \frac{7^5 \cdot 353^5 \cdot 8897857 \cdot 47113439}{2^{57} \cdot 3^{39} \cdot 19^3}$ $i_5 = \frac{5^2 \cdot 7^4 \cdot 53 \cdot 61 \cdot 353^4 \cdot 1414211 \cdot 162129559}{2^{53} \cdot 3^{37} \cdot 19^3}$ $i_6 = \frac{5 \cdot 7^3 \cdot 17 \cdot 131 \cdot 353^3 \cdot 6821753 \cdot 579475796821}{2^{51} \cdot 3^{36} \cdot 19^3}$
X^F_{2436}	$i_1 = \frac{683317^9}{2^{77} \cdot 3^{32} \cdot 7^6 \cdot 13^{14} \cdot 29^3}$ $i_2 = \frac{11 \cdot 31 \cdot 683317^7 \cdot 4586347}{2^{79} \cdot 3^{32} \cdot 7^5 \cdot 13^{14} \cdot 29^3}$ $i_3 = \frac{17 \cdot 43^2 \cdot 53 \cdot 1747 \cdot 683317^6 \cdot 5567211887}{2^{69} \cdot 3^{29} \cdot 7^6 \cdot 13^{14} \cdot 29^3}$ $i_4 = \frac{419 \cdot 647 \cdot 683317^5 \cdot 17493709 \cdot 7511015087}{2^{67} \cdot 3^{28} \cdot 7^4 \cdot 13^{14} \cdot 29^3}$ $i_5 = \frac{47 \cdot 199 \cdot 147937 \cdot 683317^4 \cdot 7244515610259779411941}{2^{63} \cdot 3^{25} \cdot 7^6 \cdot 13^{14} \cdot 29^3}$ $i_6 = \frac{5^2 \cdot 31 \cdot 199 \cdot 683317^3 \cdot 869616719123 \cdot 23481259720011791}{2^{61} \cdot 3^{22} \cdot 7^3 \cdot 13^{14} \cdot 29^3}$

Kurve	Invarianten
X^P_{2624}	$i_1 = \frac{-3733^9}{2^{105}\cdot 3^{27}\cdot 41^3}$ $i_2 = \frac{-5\cdot 3733^7\cdot 406177}{2^{107}\cdot 3^{29}\cdot 41^3}$ $i_3 = \frac{-7\cdot 149\cdot 3733^6\cdot 16879\cdot 167393}{2^{97}\cdot 3^{24}\cdot 41^3}$ $i_4 = \frac{-5^3\cdot 103\cdot 199\cdot 743\cdot 3733^5\cdot 8299073}{2^{95}\cdot 3^{25}\cdot 41^3}$ $i_5 = \frac{-3733^4\cdot 405401\cdot 27712897\cdot 133880407}{2^{91}\cdot 3^{23}\cdot 41^3}$ $i_6 = \frac{-5\cdot 1999\cdot 3733^3\cdot 443533\cdot 46191865920463}{2^{89}\cdot 3^{22}\cdot 41^2}$
X^S_{2624}	$i_1 = \frac{-3733^9}{2^{105}\cdot 3^{27}\cdot 41^3}$ $i_2 = \frac{-5\cdot 3733^7\cdot 406177}{2^{107}\cdot 3^{29}\cdot 41^3}$ $i_3 = \frac{-7\cdot 149\cdot 3733^6\cdot 16879\cdot 167393}{2^{97}\cdot 3^{24}\cdot 41^3}$ $i_4 = \frac{-5^3\cdot 103\cdot 199\cdot 743\cdot 3733^5\cdot 8299073}{2^{95}\cdot 3^{25}\cdot 41^3}$ $i_5 = \frac{-3733^4\cdot 405401\cdot 27712897\cdot 133880407}{2^{91}\cdot 3^{23}\cdot 41^3}$ $i_6 = \frac{-5\cdot 1999\cdot 3733^3\cdot 443533\cdot 46191865920463}{2^{89}\cdot 3^{22}\cdot 41^2}$
X^S_{3179}	$i_1 = \frac{7^9}{2^{44}\cdot 3^{27}\cdot 11^3\cdot 17^4}$ $i_2 = \frac{-7^7\cdot 59}{2^{48}\cdot 3^{29}\cdot 11^3\cdot 17^3}$ $i_3 = \frac{5\cdot 7^6\cdot 157\cdot 283}{2^{35}\cdot 3^{24}\cdot 11^3\cdot 17^4}$ $i_4 = \frac{-7^5\cdot 13\cdot 16456963}{2^{36}\cdot 3^{25}\cdot 11^3\cdot 17^4}$ $i_5 = \frac{7^4\cdot 111770067821}{2^{34}\cdot 3^{23}\cdot 11^3\cdot 17^4}$ $i_6 = \frac{-7^3\cdot 37\cdot 131\cdot 181\cdot 101419}{2^{32}\cdot 3^{22}\cdot 11^3\cdot 17^4}$
X^T_{3179}	$i_1 = \frac{7^9}{2^{44}\cdot 3^{27}\cdot 11^3\cdot 17^4}$ $i_2 = \frac{-7^7\cdot 59}{2^{48}\cdot 3^{29}\cdot 11^3\cdot 17^3}$ $i_3 = \frac{5\cdot 7^6\cdot 157\cdot 283}{2^{35}\cdot 3^{24}\cdot 11^3\cdot 17^4}$ $i_4 = \frac{-7^5\cdot 13\cdot 16456963}{2^{36}\cdot 3^{25}\cdot 11^3\cdot 17^4}$ $i_5 = \frac{7^4\cdot 111770067821}{2^{34}\cdot 3^{23}\cdot 11^3\cdot 17^4}$ $i_6 = \frac{-7^3\cdot 37\cdot 131\cdot 181\cdot 101419}{2^{32}\cdot 3^{22}\cdot 11^3\cdot 17^4}$
X^I_{3318}	$i_1 = \frac{5039^9}{2^{68}\cdot 3^{26}\cdot 7^5\cdot 11^{14}\cdot 79^3}$ $i_2 = \frac{5039^7\cdot 108037997}{2^{72}\cdot 3^{27}\cdot 7^5\cdot 11^{14}\cdot 79^3}$ $i_3 = \frac{5\cdot 5039^6\cdot 26723\cdot 4704853}{2^{55}\cdot 3^{22}\cdot 7^5\cdot 11^{14}\cdot 79^3}$ $i_4 = \frac{431\cdot 5039^5\cdot 34877\cdot 233430233}{2^{53}\cdot 3^{22}\cdot 7^5\cdot 11^{14}\cdot 79^3}$ $i_5 = \frac{5\cdot 17\cdot 5039^4\cdot 6682507101602677}{2^{44}\cdot 3^{20}\cdot 7^3\cdot 11^{14}\cdot 79^3}$ $i_6 = \frac{2267\cdot 5039^3\cdot 92581\cdot 8103353\cdot 13904729}{2^{42}\cdot 3^{20}\cdot 7^3\cdot 11^{14}\cdot 79^3}$

Kurve	Invarianten
X^K_{3400}	$i_1 = \frac{653^9 \cdot 220013^9}{2^{50} \cdot 3^{18} \cdot 5^6 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_2 = \frac{-7 \cdot 653^7 \cdot 5279 \cdot 220013^7 \cdot 55112715491}{2^{50} \cdot 3^{20} \cdot 5^6 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_3 = \frac{653^6 \cdot 220013^6 \cdot 40874427556386814692308225 53}{2^{45} \cdot 3^{16} \cdot 5^6 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_4 = \frac{-7 \cdot 29 \cdot 653^5 \cdot 12941 \cdot 220013^5 \cdot 178118073064914663990802 6951}{2^{42} \cdot 3^{16} \cdot 5^4 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_5 = \frac{-653^4 \cdot 2803 \cdot 220013^4 \cdot 40160863 \cdot 5402404159433201 \cdot 27562324861235273}{2^{40} \cdot 3^{13} \cdot 5^6 \cdot 17^2 \cdot 59^{14} \cdot 647^{14}}$
	$i_6 = \frac{-19 \cdot 97 \cdot 653^3 \cdot 59707 \cdot 220013^3 \cdot 181323953 \cdot 6476424276449296131391207436065046 11}{2^{36} \cdot 3^{14} \cdot 5^4 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
X^Q_{3400}	$i_1 = \frac{653^9 \cdot 220013^9}{2^{50} \cdot 3^{18} \cdot 5^6 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_2 = \frac{-7 \cdot 653^7 \cdot 5279 \cdot 220013^7 \cdot 55112715491}{2^{50} \cdot 3^{20} \cdot 5^6 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_3 = \frac{653^6 \cdot 220013^6 \cdot 40874427556386814692308225 53}{2^{45} \cdot 3^{16} \cdot 5^6 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_4 = \frac{-7 \cdot 29 \cdot 653^5 \cdot 12941 \cdot 220013^5 \cdot 178118073064914663990802 6951}{2^{42} \cdot 3^{16} \cdot 5^4 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
	$i_5 = \frac{-653^4 \cdot 2803 \cdot 220013^4 \cdot 40160863 \cdot 5402404159433201 \cdot 27562324861235273}{2^{40} \cdot 3^{13} \cdot 5^6 \cdot 17^2 \cdot 59^{14} \cdot 647^{14}}$
	$i_6 = \frac{-19 \cdot 97 \cdot 653^3 \cdot 59707 \cdot 220013^3 \cdot 181323953 \cdot 6476424276449296131391207436065046 11}{2^{36} \cdot 3^{14} \cdot 5^4 \cdot 17^3 \cdot 59^{14} \cdot 647^{14}}$
X^E_{3577}	$i_1 = \frac{5^9 \cdot 37^9 \cdot 43133^9}{2^{53} \cdot 3^{30} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
	$i_2 = \frac{-5^8 \cdot 37^7 \cdot 263 \cdot 43133^7 \cdot 197689 \cdot 6021091}{2^{57} \cdot 3^{32} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
	$i_3 = \frac{5^6 \cdot 13 \cdot 37^6 \cdot 43133^6 \cdot 142702121 \cdot 25535098000501}{2^{43} \cdot 3^{28} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
	$i_4 = \frac{5^5 \cdot 17 \cdot 37^5 \cdot 577 \cdot 43133^5 \cdot 3563719 \cdot 164875199 \cdot 160402791737}{2^{39} \cdot 3^{28} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
	$i_5 = \frac{-5^4 \cdot 13^2 \cdot 37^4 \cdot 43133^4 \cdot 411537604667032828532884132805 89099}{2^{33} \cdot 3^{24} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
	$i_6 = \frac{-5^3 \cdot 37^3 \cdot 43133^3 \cdot 688333 \cdot 28685999 \cdot 3031471393386674295606558437642759}{2^{36} \cdot 3^{26} \cdot 7^8 \cdot 11^{14} \cdot 73^3 \cdot 101^{14}}$
X^{AA}_{3718}	$i_1 = \frac{13^3 \cdot 441713^9}{2^{105} \cdot 3^{27} \cdot 11^4 \cdot 23^{14}}$
	$i_2 = \frac{-7 \cdot 13^3 \cdot 859 \cdot 441713^7 \cdot 3514123}{2^{107} \cdot 3^{29} \cdot 11^4 \cdot 23^{14}}$
	$i_3 = \frac{13^2 \cdot 449 \cdot 4463 \cdot 6211 \cdot 441713^6 \cdot 1913257757}{2^{97} \cdot 3^{24} \cdot 11^4 \cdot 23^{14}}$
	$i_4 = \frac{7^2 \cdot 13^2 \cdot 557 \cdot 1327 \cdot 441713^5 \cdot 321037206283012393}{2^{95} \cdot 3^{25} \cdot 11^4 \cdot 23^{14}}$
	$i_5 = \frac{13^2 \cdot 47 \cdot 441713^4 \cdot 3427397 \cdot 20815969 \cdot 31870960750395253}{2^{91} \cdot 3^{23} \cdot 11^4 \cdot 23^{14}}$
	$i_6 = \frac{7 \cdot 13 \cdot 31 \cdot 887 \cdot 4483 \cdot 441713^3 \cdot 1767307 \cdot 8477687 \cdot 45150242491501417}{2^{89} \cdot 3^{22} \cdot 11^4 \cdot 23^{14}}$
X^O_{3757}	$i_1 = \frac{5^9 \cdot 17^6 \cdot 37^9 \cdot 14537^9}{2^{53} \cdot 3^{27} \cdot 7^{14} \cdot 13^3 \cdot 409^{14}}$
	$i_2 = \frac{-5^7 \cdot 17^5 \cdot 37^7 \cdot 59 \cdot 8867 \cdot 14537^7 \cdot 109899089}{2^{57} \cdot 3^{29} \cdot 7^{14} \cdot 13^3 \cdot 409^{14}}$
	$i_3 = \frac{5^7 \cdot 17^4 \cdot 37^6 \cdot 14537^6 \cdot 33704049305154849133}{2^{42} \cdot 3^{24} \cdot 7^{12} \cdot 13^3 \cdot 409^{14}}$
	$i_4 = \frac{-5^5 \cdot 17^5 \cdot 37^5 \cdot 14537^5 \cdot 16277294161078469874669 29}{2^{41} \cdot 3^{25} \cdot 7^{11} \cdot 13^3 \cdot 409^{14}}$
	$i_5 = \frac{5^4 \cdot 17^3 \cdot 37^4 \cdot 2699 \cdot 14537^4 \cdot 415133 \cdot 22251582641503569502656113}{2^{36} \cdot 3^{23} \cdot 7^{11} \cdot 13^3 \cdot 409^{14}}$
	$i_6 = \frac{5^3 \cdot 17^2 \cdot 37^3 \cdot 139 \cdot 14537^3 \cdot 28021271 \cdot 13194547068301 \cdot 1569599695257109441}{2^{36} \cdot 3^{22} \cdot 7^9 \cdot 13^3 \cdot 409^{14}}$

Kurve	Invarianten
X^O_{3924}	$i_1 = \frac{7^9 \cdot 167^9}{2^{37} \cdot 3^{42} \cdot 5^{12} \cdot 109^3}$
	$i_2 = \frac{-7^8 \cdot 103 \cdot 167^7 \cdot 2287}{2^{41} \cdot 3^{44} \cdot 5^{12} \cdot 109^3}$
	$i_3 = \frac{7^7 \cdot 11 \cdot 167^6 \cdot 3971210053}{2^{35} \cdot 3^{39} \cdot 5^{12} \cdot 109^3}$
	$i_4 = \frac{-7^5 \cdot 113 \cdot 167^5 \cdot 787 \cdot 17657 \cdot 52301}{2^{33} \cdot 3^{40} \cdot 5^{11} \cdot 109^3}$
	$i_5 = \frac{7^4 \cdot 163 \cdot 167^4 \cdot 68819 \cdot 1639520011631}{2^{32} \cdot 3^{38} \cdot 5^{11} \cdot 109^3}$
	$i_6 = \frac{7^3 \cdot 11 \cdot 167^3 \cdot 307 \cdot 65484401 \cdot 1299470603113}{2^{31} \cdot 3^{37} \cdot 5^{12} \cdot 109^3}$
X^Q_{3969}	$i_1 = \frac{5^4}{2^{53} \cdot 3^9 \cdot 7^3}$
	$i_2 = \frac{5 \cdot 17}{2^{57} \cdot 3^{12} \cdot 7^3}$
	$i_3 = \frac{5 \cdot 3821}{2^{42} \cdot 3^8 \cdot 7^3}$
	$i_4 = \frac{17 \cdot 8363}{2^{41} \cdot 3^9 \cdot 5 \cdot 7^3}$
	$i_5 = \frac{5^2 \cdot 313}{2^{38} \cdot 3^6 \cdot 7^3}$
	$i_6 = \frac{-19 \cdot 83 \cdot 11119}{2^{36} \cdot 3^7 \cdot 5^2 \cdot 7^3}$

Literaturverzeichnis

[1] L. M. Adleman, J. DeMarrais, and M-D. Huang. A subexponential algorithm for discrete logarithms in the rational subgroup of the Jacobian of a hyperelliptic curve over a finite field. In *Algorithmic Number Theory Symposium - 1994*, volume 877 of *LNCS*, pages 28–40. Springer, 1994.

[2] S. Arita. An Addition Algorithm in Jacobian of $C_{3,4}$ Curve. In *Information Security and Privacy, ACISP 2003*, volume 2727 of *LNCS*, pages 93–105. Springer, 2003.

[3] A. Atkin and J. Lehner. Hecke operators on $\Gamma_0(m)$. *Math. Ann.*, 185:134–160, 1970.

[4] R. M. Avanzi, G. Frey, T. Lange, and R. Oyono. On using expansions to the base of -2. *Inter. J. of. Comp. Math.*, 81(4):403–406, 2004.

[5] M. H. Baker, E. González-Jiménez, J. González, and Bjorn Poonen. Finiteness Result for Modular Curves of Genus at least 2. Available on `http://math.berkeley.edu/~poonen/papers/finiteness.pdf`, 2003.

[6] A. Basiri, A. Enge, J-C. Faugère, and N. Gürel. Implementing the Arithmetic of $C_{3,4}$ Curves. In *Algorithmic Number Theory Symposium - ANTS-VI*, volume 3076 of *LNCS*, pages 87–101. Springer, 2004.

[7] A. Basiri, A. Enge, J-C. Faugère, and N. Gürel. The arithmetic of Jacobian groups of superelliptic cubics. *Math. Comp.*, 74:389 – 410, 2005.

[8] J. Basmaji. *Ein Algorithmus zur Berechnung von Hecke-Operatoren und Anwendung auf modulare Kurven.* PhD thesis, Institut für Experimentelle Mathematik Essen, 1996.

[9] M. Bauer. A subexponential algorithm for solving the discrete logarithm problem in the Jacobian of high genus hyperelliptic curves over arbitrary finite fields. preprint, 1998.

[10] D. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[11] L. Caporaso and E. Sernesi. Recovering plane curves from their bitangents. *J. Alg. Geom.*, 2:225–244, 2003.

[12] S. A. Cook. On the minimum computation time of functions. Master's thesis, Harvard University, Boston, Massachusetts USA, 1966.

[13] O. Debarre. *Tores et variétés abéliennes complexes.* Cours spécialisés 6, collection SMF, 1999.

[14] P. Deligne. Formes modulaires et réprésentations l-adic. *Sem. Bourbaki, 21e Année 1968/69 n. 355, Lect. Notes in Math.*, 179:139–172, 1971.

[15] P. Deligne. La conjecture de Weil I. *Inst. Hautes Études Sci. Publ. Math.*, 43:273–307, 1974.

[16] P. Deligne and D. Mumford. The irreducibility of the space of curves of given genus. *Publ. Math. IHES*, 36:75–110, 1969.

[17] J. Denef and F. Vercauteren. Counting points on C_{ab} curves using Monsky-Washnitzer cohomology, 2003. preprint.

[18] J. Dixmier. On the projective Invariants of quartic plane curves. *Advances in Math.*, 64:279–304, 1987.

[19] I. Dolgachev. Topics in classical algebraic geometry, part I. Available on `http://www.math.lsa.umich.edu/~idolga/lecturenotes.html`, 2003.

[20] M. Eichler. Quaternäre quadratische Formen und die Riemannsche Vemutung für die Kongruenzzetafunktion. *Arch. Math.*, 5:355–366, 1954.

[21] A. Enge. *Hyperelliptic Cryptosystems.* PhD thesis, Universität Augsburg, 2000.

[22] A. Enge. How to distinguish hyperelliptic curves in even characteristic. *Public -key Cryptography and computational number theory (Warsaw, 2000)*, pages 49–58, 2001.

[23] A. Enge. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. *Mathematics of Computation*, 71(238):729–742, 2002.

[24] S. Flon and R. Oyono. Fast arithmetic on Jacobians of Picard curves. In *Public Key Cryptography - PKC 2004*, volume 2947 of *LNCS*, pages 55–68. Springer, 2004.

[25] S. Flon, R. Oyono, and C. Ritzenthaler. Fast Addition on Non-hyperelliptic genus 3 curves. Preprint, available on `http://http://eprint.iacr.org/2004`, 2004.

[26] G. Frey and M. Müller. Arithmetic of modular curves and applications. In *Algorithmic Algebra and Number Theory*, pages 11–48. Ed. Matzat et al., Springer-Verlag, Berlin, 1999.

[27] R. P. Gallant, J. L. Lambert, and S. A. Vanstone. Faster point multiplication on elliptic curves with efficient endomorphisms. In *Advances in Cryptology – Crypto'2001*, volume 2139 of *LNCS*, pages 190–200. Springer, 2001.

[28] P. Gaudry. An algorithm for solving the discrete log problem on hyperelliptic curves. In *Advances in Cryptology - Eurocrypt'2000*, volume 1807 of *LNCS*, pages 19–34. Springer, 2000.

[29] P. Gaudry. *Algorithmique des courbes hyperelliptiques et Applications à la cryptologie*. PhD thesis, École polytechnique, 2000.

[30] M. Gonda, K. Matsuo, K. Aoki, J. Chao, and S. Tsujii. Improvements of addition algorithm on genus 3 hyperelliptic curves and their implementations. In *SCIS 2004*, 2004.

[31] J. González, J. Guàrdia, and V. Rotger. Abelian surfaces of GL_2-type as Jacobians of curves. *Acta Arithmetica*, 116(3):263–287, 2005.

[32] E. González-Jiménez. *Curvas hiperelípticas Modulares*. PhD thesis, Universitat Autònoma de Barcelona, 2001.

[33] E. González-Jiménez and J. González. Modular curves of genus 2. *Math. comp.*, 72:397–418, 2003.

[34] E. González-Jiménez, J. González, and J. Guàrdia. Computations on Modular Jacobian Surfaces. In *Lecture Notes in Comput. Sci. (2369)*, pages 189–197. Springer, 2002.

[35] E. González-Jiménez and J. Guàrdia. MAV, modular abelian varieties for MAGMA. Available on `http://andurileupvg.upc.es/~gaurdia`, 2001.

[36] E. Gottschling. Explizite Bestimmung der Randflächen des Fundamentalbereiches der Modulgruppe zweiten grades. *Duke Math. J.*, 76/3:809–884, 1994.

[37] J. Guàrdia. Jacobian nullwerte and algebraic equations. *Journal of Algebra*, 253:112–132, 2002.

[38] J. Guàrdia. Jacobian nullwerte, periods and symmetric equations for hyperelliptic curves, 2004. preprint.

[39] C. Guyot, K. Kaveh, and V. M. Patankar. Explicit algorithm for the arithmetic on the hyperelliptic Jacobians of genus 3. *J. Ramanujan Math. Soc.*, 19:75–115, 2004.

[40] R. Hartshorne. *Algebraic geometry*, volume 52. Springer-Verlag, GTM, 1977.

[41] F. Hess. *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern.* PhD thesis, TU Berlin, 1999.

[42] J.W.P Hirschfeld, G. Korchmáros, and L. Storme. Arcs and caps in projective spaces. Available on `http://cage.ugent.be/~fdc/intensivecourse/james.ps`.

[43] M. Homma. Funny plane curves in characteristic $p > 0$. *Comm. Algebra*, 15:1469–1501, 1987.

[44] E. W. Howe. Plane quartics with Jacobians isomorphic to a hyperelliptic Jacobian. *Proc. of the AMS*, 129(6):1647–1657, 2000.

[45] M-D. Huang and D. Ierardi. Efficient algorithms for the Riemann-Roch problem and for addition in the Jacobian of a curve. *J. of symb. comp.*, 18:519–539, 1994.

[46] G. Humbert. Sur les fonctions abéliennes singulières (deuxieme mémoire). *J. Math. Pures Appl.*, 5(6):279–386, 1900.

[47] J. Igusa. Kroneckerian model of fields of elliptic modular functions. *Amer. J. Math.*, 81:561–577, 1959.

[48] J.-I. Igusa. *Theta functions*, volume 194 of *Die Grundlehren der mathematischen Wissenschaften*. Springer Verlag, 1972.

[49] A. Karatsuba and Y. Ofman. Multiplication of multidigit numbers on Automata. *Sov. Phys. Dokl. (Engl. translation)*, 7(7):595–596, 1963.

[50] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *J. Ramanujan Math. Soc.*, 16(4):323–338, 2001.

[51] K. Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 33(4):333–357, 2004.

[52] N. Koblitz. Elliptic curve cryptosystems. *Math. Comp.*, 48(177):203–209, 1987.

[53] K. Koike and A. Weng. Construction of CM-Picard curves. *Math. Comp.*, 74 (249):499–518, 2004.

[54] J. Kuroki, M. Gonda, K. Matsuo, J. Chao, and S. Tsujii. Fast genus three hyperelliptic curve cryptosystems. In *SCIS 2002*, 2002.

[55] S. Lang. Abelian varieties. *Interscience Tracts in Pure and Applied Mathematics*, 7, 1959.

[56] H. Lange. Abelian varieties with several principal polarizations. *Duke Math. J.*, 55(3):617–628, 1987.

[57] H. Lange and W. Ruppert. Complete systems of addition laws on abelian varieties. *Invent. Math.*, 79:603–610, 1985.

[58] T. Lange. Formulae for Arithmetic on Genus 2 Hyperelliptic Curves. *J. AAECC*, 15(5):295–328, 2005.

[59] D. Lehavi. *Bitangents and two level structures for curves of genus* 3. PhD thesis, Hebrew University of Jerusalem, 2002.

[60] MAGMA. Computational Algebra System. Available on `http://magma.maths.usyd.edu.au/magma/`.

[61] K. Matsuo, J. Chao, and S. Tsujii. Fast genus two hyperelliptic curve cryptosystems. Technical report, IEICE, 2001. ISEC2001-31.

[62] V.S. Miller. The use of elliptic curves in cryptography. In *Advances in cryptology-CRYPTO '85*, volume 218 of *LNCS*, pages 417–426, Santa Barbara, California, 1986. Springer-Verlag.

[63] J-S. Milne. Abelian varieties. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 103–150. Springer, 1986.

[64] J-S. Milne. Jacobian varieties. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer, 1986.

[65] R. Miranda. *Algebraic curves and Riemann surfaces*, volume 5. Graduates studies in Mathematics, 1995.

[66] S. Miura. Algebraic geometric codes on certain plane curves. *IEICE*, J75 - A (11):1735–1745. In Japanese, 1992.

[67] D. Mumford. On the equations defining abelian varieties. *Invent. Math.*, 1:287–354, 1966.

[68] D. Mumford. *Geometric invariant theory*. Springer, 1982.

[69] D. Mumford. *Tata lectures on theta I*, volume 28 of *Progress in mathematics*. Birkhaüser, 1983.

[70] D. Mumford. *Tata lectures on theta II*, volume 43 of *Progress in mathematics*. Birkhaüser, 1984.

[71] G. Orzech and M. Orzech. *Plane algebraic curves*, volume 61. Pure and Applied Math., New-York, 1981.

[72] J. Pelzl, T. Wollinger, J. Guajardo, and C. Paar. Hyperelliptic curves cryptosystems: closing the performance gap to elliptic curves. In *Cryptographic Hardware and Embedded Systems - CHES 2003*, volume 2779 of *LNCS*, pages 351–365. Springer, 2003.

[73] C. Poor. On the hyperelliptic locus. *Duke Math. J.*, 76/3:809–884, 1994.

[74] E. Reinaldo-Barreiro, J. Estrada-Sarlabous, and J-P. Cherdieu. Efficient reduction on the Jacobian variety of Picard curves. In *Coding theory, cryptography, and related areas*, volume 877, pages 13–28. Springer, 1998.

[75] K. A. Ribet. Galois Representations attached to Eigenforms with Nebentypus. In *Lecture Notes in Mathematics*, pages 17–52. Berlin, Heidelberg New york: Springer, 1977.

[76] K. A. Ribet. Twists of Modular Forms and Endomorphisms of Abelian Varieties. *Math. Ann.*, 253:43–62, 1980.

[77] B. Riemann. Sur la théorie des fonctions abéliennes. *Oeuvres de Riemann, 2nd edition*, page 487, 1898.

[78] C. Ritzenthaler. *Problèmes arithmétiques relatifs à certaines familles de courbes sur les corps finis*. PhD thesis, Université Paris 7, 2003.

[79] C. Ritzenthaler. Point counting on genus 3 non hyperelliptic curves. In *Algorithmic Number Theory Symposium - ANTS-VI*, volume 3076 of *LNCS*, pages 379–394. Springer, 2004.

[80] M. Rosen. Abelian varieties over $\mathbb{C}$. In Cornell G. and J.H. Silverman, editors, *Arithmetic Geometry*, pages 167–212. Springer, 1986.

[81] B. Schoeneberg. *Elliptic modular functions*, volume 203. Springer-Verlag, Grundlehren Math. Wiss., 1974.

[82] T. Shaska and J. L. Thompson. On the generic curve of genus 3. *Contemporary. Math.*, 369:233–244, 2005.

[83] G. Shimura. Correspondances modulaires et les fonctions ζ de courbes algébriques. *J. Math. Soc. Japan*, 10:1–28, 1958.

[84] G. Shimura. *Introduction to the arithmetic Theory of Automorphic Functions*. Iwanami - Princeton, 1971.

[85] G. Shimura. On elliptic curves with complex multiplication as factors of the Jacobians of modular function fields. *Nagoya Math. J.*, 43:199–208, 1971.

[86] G. Shimura. Class fields over real quadratic fields and Hecke operators. *Ann. of Math.*, 95:130–190, 1972.

[87] G. Shimura. On the factors of the jacobian variety of a modular function field. *J. Math. Soc. Japan*, 25(3):523–544, 1973.

[88] G. Shimura and Y. Taniyama. Complex multiplication of abelian varieties and its applications to number theory. *Math. Soc. Japan*, 6, 1961.

[89] A.-M. Spallek. *Kurven vom Geschlecht* 2 *und ihre Anwendung in Public-key-Kryptosystemen*. PhD thesis, Institut für Experimentelle Mathematik Essen, 1994.

[90] A. Stein. Sharp upper bounds for arithmetic in hyperelliptic function fields. *J. Ramanujan Math. Soc*, 16(2):119–203, 2001.

[91] W. A. Stein. The Modular Forms Explorer. Software, available on `http://modular.ucsd.edu/mfd/mfe/`.

[92] A. R. Taylor and A. Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[93] N. Thériault. Index calculus attack for hyperelliptic curves of small genus. In *Asiacrypt 2003*, LNCS, pages 75–92. Springer, 2003.

[94] F. Torres. The approach of Stöhr-Voloch to the Hasse-Weil bound with applications to optimal curves and plane arcs. Available on `http://arxiv.org/abs/math.AG/0011091`, 2000.

[95] E. Volcheck. Computing in the Jacobian of a plane algebraic curve. In Adleman, editor, *ANTS-I*, volume 877, pages 221–233. Springer-Verlag, 1994.

[96] X. Wang. 2-dimensional simple factors of $J_0(N)$. *Manuscr. Math.*, 87:179–197, 1995.

[97] H-J. Weber. *Algorithmische Konstruktion hyperelliptischer Kurven mit kryptographischer Relevanz und einem Endomorphismenring echt größer als* $\mathbb{Z}$. PhD thesis, Institut für Experimentelle Mathematik Essen, 1997.

[98] A. Weil. Zum Beweis des Torellischen Satzes. *Nach. der Akad. der Wiss. Göttingen, Math. Phys. Klasse*, pages 33–53, 1957.

[99] A. Weng. *Konstruktion kryptographisch geeigneter Kurven mit komplexer Multiplikation*. PhD thesis, Institut für Experimentelle Mathematik Essen, 2001.

[100] A. Weng. Generation of random Picard Curves for Cryptography. Available on `http://eprint.iacr.org/2004/285.pdf`, 2004. preprint.

[101] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.